Luis Diego Zúñiga Mayorga

Network Selection Optimization in a Secured Mobile IP Data Overlay System

School of Electrical Engineering

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Technology.
Espoo, November 2015

Thesis supervisor:
Prof. Jukka Manner

Thesis instructor:
Ph.D. Roman Pichna

Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Luis Diego Zuniga Mayorga

Title: Network Selection Optimization in a Secured Mobile IP Data Overlay System

Date: 12.11.2015 Language: English Pages: 65+13

Department of Communications and Networking

Professorship: Networking Technologies Code: S-38

Supervisor: Prof. Jukka Manner, PhD, Aalto University

Instructor: Roman Pichna, PhD, Airbus Defense and Space

The purpose of this thesis to so solve a limitation in the switchover mechanism of a Mobile IP (MIP) client device where it fails to change the active Mobile IP leg in a scenario where the current used path is just marginally good. The MIP client is a Cisco 819 router that provides internet connectivity to end users via an internal radio interface to a public Mobile Network Operator (MNO) and an external modem connected via an Ethernet port. When Mobile IP fails to properly select the active leg, the end user's experience detriments and is unable to continue normal operation, this is why a mechanism is needed to probe the available networks and to select the best one for the end user. This work studies different vertical handover mechanisms that could be used in this type of environments where not only, not all the participants of the handover selection are radio interfaces; as in this case one interface is an external device, but also where most of the physical information of an interface is not available to use as part of a handover algorithm.

This thesis proposes three different mechanisms to choose the best available network at any given time to complement the Mobile IP operation. The first mechanism is based on Round-Trip-Time (RTT), the next mechanism uses immediate throughput as the metric for the network selection and the final proposal is a muti-attribute algorithm where very poor networks will be filtered by their larger RTT values first and only then will the immediate available throughput will be measured.

The results show that the three mechanisms provided a decrease in the downtime experienced by the end user where the RTT-based algorithm had the lowest increase in performance and the immediate-throughput-based proposal had the highest increase. The multi-attribute mechanism; while not top performing in terms of less downtime, significantly reduced the amount of time it took to select the new network and thus provides better end user experience.

Keywords: Mobile IP, Vehicular Networks, Mobile Networks, Always Best Connected, Vertical Handover Algorithms

Acknowledgment

I am truly grateful and will always appreciate my instructor, *Ph.D Roman Pichna*, his support and encouragement made pushed me into completing this thesis, while his constant challenges and wisdom helped me understand and focus; not only for this thesis, but for life itself. Thank you very much, Roman.

To my friends here in Finland, who helped me overcome being so far away from home, you will always have my thanks.

To my family and friends back home who always encouraged me and always worried about me, this has been a long journey but they have helped me so much throughout all this time, this would not have been possible without all your concern.

Familia, los amo a todos.

Luis Diego Zúñiga Mayorga

Espoo, 10.11.2015

Table of contents

Abbreviations and Acronyms

ABC	Always Best Connected
AHP	Analytic Hierarchy Process
ANDSF	Access network discovery and selection function
BER	Bit Error Rate
BGP	Border Gateway Protocol
CCoA	Collocated Care of Address
CIR	Carrier Interference Ratio
CoA	Care of Address
DMZ	Demilitarized Zone
EIGRP	Enhanced Interior Gateway Routing Protocol
FA	Foreign Agent
FL	Fuzzy Logic
GRA	Grey Relational Analysis
GRC	Grey Relational Coefficient
GRE	Generic Routing Encapsulation
HMAC	Hash-based Message Authentication Code
HOC	Handover Coefficient
HTTP	Hyper Text Transfer Protocol
IPinIP	IP in IP encapsulation
LMA	Local Mobility Agent
LMD	Localized Mobility Domain
MADM	Multi Attribute Decision Making
MAG	Mobile Access Gateway
MD5	Message Digest 5
MIH	Media Independent Handover
MN	Mobile Node
MTU	Maximum Transfer Unit
NAI	Network Address Identifier
NN	Neural Network
OSPF	Open Shortest Path First
PBR	Policy Based Routing
PfR	Performance-based Routing
PL	Packet Loss
PMIP	Proxy Mobile IP
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request for Comments
RIP	Routing Information Protocol
RSS	Received Signal Strength
SAW	Simple Additive Weighting
SCTP	Stream Control Transmission Protocol plus
SIP	Session Initiation Protocol
SNR	Signal to Noise Ratio
SPI	Security Parameter Index
Th	Threshold

TOPSIS	Technique for Order Preference by Similarity to Ideal Solution
URI	Unique Resource Identifier
VHO	Vertical Handover
WP	Weighted Product

List of figures

List of tables

1 Introduction

Broadband communication have reached a point in terms of ubiquity; that users may rely on them for their mission critical applications, added to the reliability and coverage of the average mobile network; there is also redundancy in terms of access, with technologies such as EGRPS, HSPA, WCDMA, LTE or, WiFi serving remote mobile wireless access to the corporate network. Another advantage of these access means would be that the mobile users can now get increased bandwidth, comparable to wired internet access.

With these benefits in mind is that Airbus is designing the architecture for a Secure Mobile Data Overlay System; in which users can experience higher throughput, network reliability and secured communication while roaming between networks. This architecture has been conceived with vehicular networks on sight; granting a platform in which any application could function as though as it were connected directly inside the home network, this can be achieved with the help of Mobile IP and IPSec tunnels.

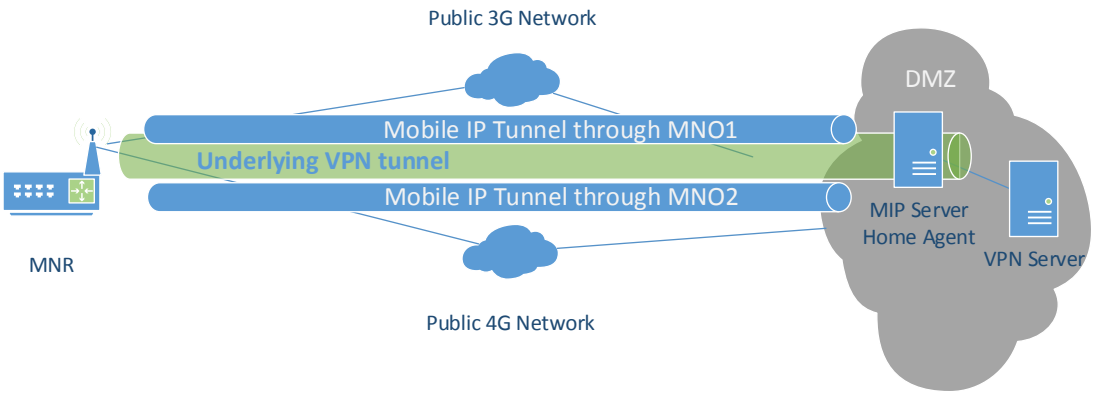

Figure 1-1 - Secured Mobile IP Data Overlay System.

As shown in Figure 1-1, the system will make use of Mobile IP (MIP) in order to create a secured mobile tunnel between the mobile nodes and the home agent in the HQ through each of the available interfaces, this alone provides uninterrupted access to the corporate network; however, truly secured and encrypted communication is given once the IPsec tunnel is established between the mobile router and the VPN server. The project will make use solely of Commercial Off-the-Shelf (COTS) devices in order to have the devices interoperate with as many vendors as possible.

1.1 Challenges

By design, a specific vendor was selected to be used as the center of this architecture; as such, we're restricted by the functionality of the COTS devices we're using. The MNO (Mobile Network Operator) network is out of reach as it was decided to use readily available USIMs that make use of public infrastructure. In most of the cases, one of the MNOs will be preferred as they may offer better opportunities for the users; as such, network selection should somehow favor this network. Network coverage may be a constraint in some cases or

areas. The selected COTS products and software is unable to react based on the performance of the network. The objective of this thesis is to overcome these limitations by investigating and implementing different network selection algorithms without changing available hardware or software, but only by means of changing the devices' configuration and/or implementing scripts in the terminals.

Due to the security-enclosed environment in which this network needs to be implemented, there are certain challenges that need to be overcome when solving the case at hand. These limitations come from the side of the end-user, the providing organization and the devices used. In terms of end user and provider originated limitations, one of them is the fact that the Home Agent and VPN Server are located in a secured facility hence these devices will be inaccessible and won't be involved in the elaboration of the final algorithm. Continuing, there is a limit of 1 on how many external modems will be used on the Cisco 819 routers and, since the public MNO networks will be used, there can't be any tampering of the RAN (Radio Access Network). Concerning the device itself, there will be the following limitations: the Cisco 819 has proprietary OS, the only available way to create custom applications is through Cisco's Tool Command Language (TCL) [1], the router itself is quite limited in terms of resources, the external modems will be connected through Ethernet ports either 100BASE-TX or 1000BASE-TX and it is not possible to access these modems or obtain any information from them.

While the MIP protocol provides a quick handover mechanism to a new network whenever the Mobile Node Router (MNR) loses connectivity to its Home Agent (HA) through the active leg, there are occasions where the data rate that the users need is limited due to low Signal-to-Noise Ratio (SNR) or GPRS access only, as examples. In such situations is where basic mobile IP functionality is not enough and an additional mechanism is needed to select the best network when the available data rate is not enough. Airbus would like to investigate if it is possible to extend said tool to work at all times so that the user is always using the best available network in terms of immediate throughput.

1.2 Solution

This project focuses on the MNR as the rest of the components are out of reach for configuration and therefore are out of the scope for the thesis. The MNR itself it is a Commercial Off-The-Shelf (COTS), a Cisco model 819 with a single 3G radio. Because of the lack of extra radio interfaces, the MNR will have attached to it at least one more modem to be able to make use of the Mobile IP features. The mobile router itself will have its own network (see Figure 1-2) using the internal 3G antenna as one of the MIP legs and, having collocated care-of-addresses destined to external modems, as alternatives to establish the tunnel to the Home Agent. This new contraption connected to our Mobile IP Client router will be only used as a generalization in this thesis because the only function of this external device will be to provide access to an additional MNO network apart from the one directly attached to the Cisco 819. Henceforward any terms referring to the MNR will encompass both the 819 router and the external modems attached to it.

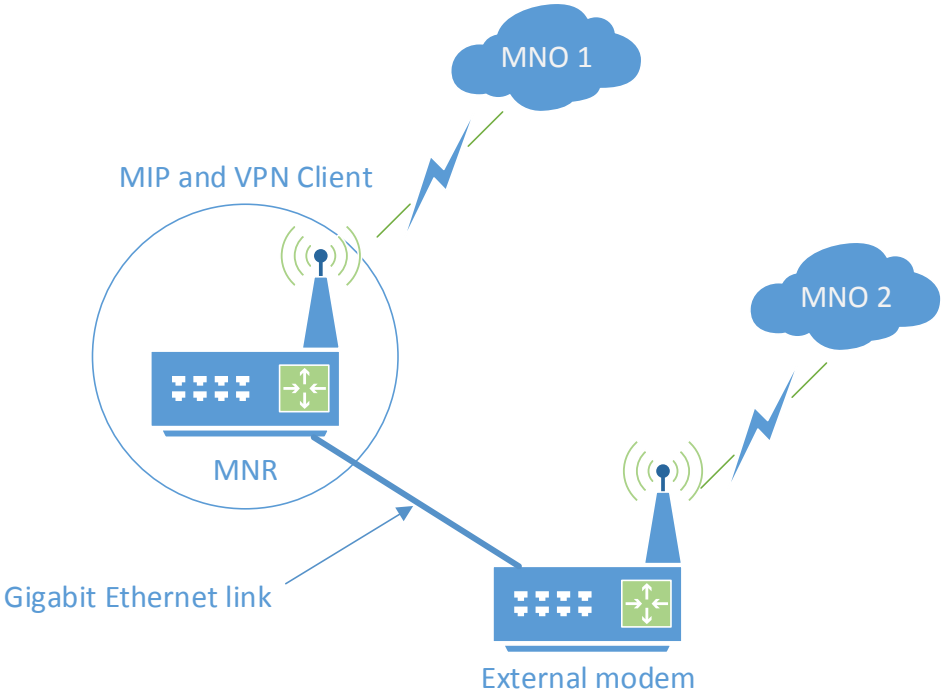

Figure 1-2 - Physical set up of Cisco Routers.

The end users will connect only to the MNR, otherwise they won't have access to the features of Mobile IP or IPSec tunneling. As a summary, the data path end users will follow will be as listed below:

1. End user generates outgoing packet.
2. MNR receives packet, matches IPSec policies and encapsulates the packet into ESP. The source IP of the ESP packets is the Home Address of the MNR.
3. IPSec process releases the packet to the routing table once again, MIP process picks it up and encapsulates it in UDP.
4. MIP releases the packet to one of its roaming interfaces while adds the missing headers, applying NAT at egress.
5. The Home Agent receives the encapsulated ESP packet in the associated to this MNR, decapsulates it and forwards it to the VPN server.
6. The VPN server will receive the ESP IPSec packet, decapsulate it and forward it out to the end-user original destination.

1.3 Result

During the data collection period one issue arose that was deemed by us as the first to solve and what we'll be aiming to aid with this solution; it is a scenario where users are static for a long period of time in an area with low throughput, i.e, LTE on coverage edge in the active interface. In this situation, the MIP tunnel will still be active but the end user will be afflicted with a much lower quality connection; however, if in this same moment an external modem

connected to the MNR, had better reception and signal quality, it is desired to sense this and switch to the better leg.

My task for this thesis was to create a program to assist the Mobile IP process in making a switch over decision, this program takes into consideration simple statistics that could be retrieved on the spot, and these are: Download and Upload rate of a file to an internet location and ICMP (Internet Control Message Protocol) round trip time (RTT). The research made helped categorize the resulting algorithms in three different ways: RTT-based selection algorithm, immediate-throughput-based selection algorithm and the multi-attribute-based selection algorithm.

The RTT-based solution proved to be not as reliable but it showed an improvement in the overall functioning of the process. The benefit of using RTT-based is that is fast to detect a failure because it only waits for the ICMP timeout and that it doesn't consume as much data resources. The immediate-throughput-based mechanism is very reliable in the sense that depending on what the desired data rate is, the filter chosen will consistently select the network that provides this value this; however, comes with a delayed response and with a greater data consumption toll. Finally, the multi-attribute algorithm allows for faster response at the cost of a bit less reliability as it will make a selection; first by comparing RTT values and then by using the immediate throughput result if the first test is non-conclusive. Overall the implemented algorithms showed an improvement over the base system in the scenario where it was most needed.

Following this work through its conclusion will see four more chapters, the next one will be an overview of the technologies; such as Mobile IP or IEEE's 802.21, that helped develop the end result. Chapter three contains: the selection of the metrics to be analyzed by the developed software, the elaboration of the algorithms to be tested as the final solution and the means of testing, the Results chapter soon afterwards displays the data taken from the experiments and compares each one of the algorithms. The final chapter explains the outcome of the experiments and whether the results meet the expectations or not.

2 Architectural Framework for Mobility

This section will go through the fundaments of failover technologies which concepts or tools will prove to be useful for this thesis. The section below will first describe the very important Mobile IP protocol which is used as the basis for the development of the solution, the following section will go on to describe what the Always Best Connected paradigm is; which some of the protocols or technologies studied here try to achieve, different protocols and technologies starting from a very basic form of mobility found in DHCP, different routing protocols, IEE 802.21, 3GGP's ANDSF and finally a few words on micromobility.

2.1 Mobile IP

Mobile IP was designed for users that require to maintain connectivity throughout multiple networks as it creates a logical link between the user equipment and a centralized location that will disregard any changes in the access technologies used by the terminal. We will describe and explain the basic concepts of Mobile IP as they will be useful for the rest of the thesis work.

2.1.1 RFCs

Mobile IP is initially described in RFC 2002 [2] by the IETF and it defines several architectural entities that the protocol makes use of, Figure 2-1 shows an overview of the function of these entities. The Home Agent (HA) will be acting as the server for Mobile IP requests and will be the termination for the Mobile IP tunnels. The HA will allow a UE in a different location to connect a Home Network directly to it by making use of this protocol, this way the home network would appear as directly connected to the HA to any traffic needing to go to the user at the Mobile Node (MN). The MN is the entity that requires to make use of Mobile IP, the tunnels should be established in this device and should have as the ultimate destination the Home Agent. The IP in the MN's interface that communicates with the Home Agent is called a Care of Address (CoA), the HA will utilize this to send the traffic to the MN's Home Address (the IP address inside the Home network). Alternatively the MN has may need or may have to use a Foreign Agent (FA) in order to establish a connection to the Home Agent, this can be used in circumstances where detailed billing is needed; as an example. If the MN is connected directly to local router without FA functioning, its CoA is called a Collocated Care of Address (CCoA); which will be used to interface directly with the HA. The RFC defines that should the MN be located outside of its own network; meaning outside of its Home Network, this device should be able to discover which HAs are available to it by making use of the ICMP Router Discovery mechanism. The HA will send ICMP Router Advertisements to the public network where the MN might be. Once the MN has learnt of a HA it may proceed to register via its CCoA or via a Foreign CoA. One aspect to notice is that if the MN is making use of a FA, every MIP that it receives from the MN, it will need to forward it the MIP HA because this will be the centralized location of all bindings in the home network.

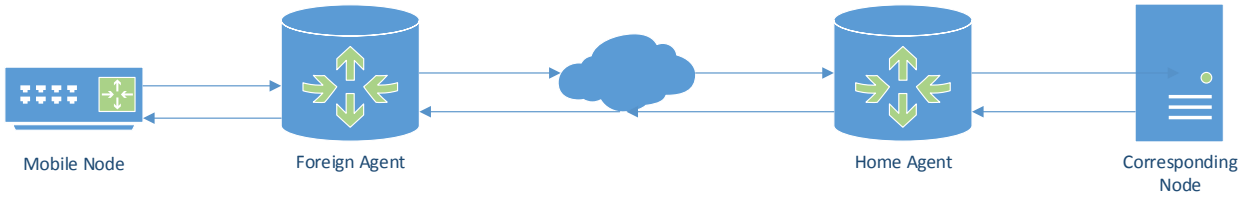

Figure 2-1 - Mobile IP architectural entities.

By default, whenever the MN moves to a different network the tunnels can be reestablished once the device knows it is been moved to a different network and receives the ICMP Router Advertisement messages through a different network, it is only then that a new connection to the HA will be established. If the MN is making use of a foreign agent, MIP messages containing the prefix of the network can be used to learn if the MN has changed locations and thus needs to send a new registration message. The RFC suggests these are not the only ways possible to learn this information but these were the options available by default.

Once the Mobile Node has learnt of at least one Home Agent it may proceed to send a registration message. This MIP requests consist of the following options: Simultaneous Bindings, Broadcast Datagrams, Decapsulation by Mobile Node, Minimal Encapsulation, GRE (Generic Routing Encapsulation) Encapsulation, Use Van Jacobson header compression and 2 reserved bits. Then it has the following fields: Home Address, Home Agent, Care-of-Address, Identification and extensions. Out of these, the MN needs to be pre-configured with a Home Address, a Network Mask and a Security Parameter Index (SPI) for identification purposes, the Home Agent address will be learnt by the advertisement protocol. Multiple Bindings and Decapsulation by Mobile Node are interesting options for us, the first one allows the MN to have several logical links to the Home Agent if device has several interfaces to send the traffic through, the latter one because it means the MN will be in charge of decapsulating the packet and therefore there should at least be a tunnel between the MIP and the MN (in this direction). If there was a FA the traffic to a Corresponding Node (CN) by default would flow MN < FA < HA < CN and MN > FA > CN, with traffic going directly to CN. If the option for the MN to decapsulate the MIP packets is set, return traffic would be: MN < HA < CN; which is the case when the MN is using CCoA.

Based on the information in the header it is possible to know that there won't be any encryption being established between the packets are there is no cypher sets being compared. MIP offers only authentication; in RFC 2002 with MD5 using prefix-suffix method and in RFC 3344 [3] HMAC-MD5 was added, every header and extension should be authenticated and the HA and MN should verify the authenticity of the messages they receive. Another security feature of Mobile IP is to keep a timestamp of every message sent or received in order to avoid replay attacks.

With the RFC 3344, several error correction mechanisms were introduced as well as the inclusion of support for Network Address Identifier (NAI), NAI which is proposed under RFC 2794 in [4] allows a MN to be recognized by a Unique Resource Identifier (URI) instead of a Home Address, this meant there was the possibility to dynamically assign Home Address to the MIP terminals, for the foreign agents as well as for the home agents this meant

they should be able to support devices with possibly the same Home Addresses as it is no longer required to pre-configure this address if there is a NAI. Another inclusion in this RFC was the support for reverse tunneling which is defined under RFC 3024 [5] and it provides a way for the MN to have symmetric and secure data flows by making the return path from the CN to MN when there is a Foreign Agent to go from MN to FA towards the HA and finally to the CN. For the foreign agent this meant that the outgoing and incoming traffic legs would be to/from the Home Agent, instead of one of them going to a different network towards the CN. The latest release of the Mobile IP RFCs, RFC 5944 [6] adds several security features and more robust mechanisms against Denial of Service, these features are not interesting for us in this environment and therefore will be left out. From this point on, it will be assumed that there is no Foreign Agent in the network and therefore the MN will make use of a CCoA, this is because foreign agents haven't been deployed in this type of environment and because it would affect the IP address allocation within the whole network.

One of the previously mentioned characteristics of Mobile IP is the ability to create a tunnel between the HA and the MN; however, the way this tunnel is created varies depending on what the MN needs. In RFC 2002 IP in IP was the default choice for tunneling and it is described under RFC 2003 [7]. This document describes the process of encapsulation an IP packet inside another IP packet with protocol type 4, and it will follow the basic flow as in Figure 2-2; however if a Foreign Agent is being used then the MN may choose not to encapsulate traffic to the FA.

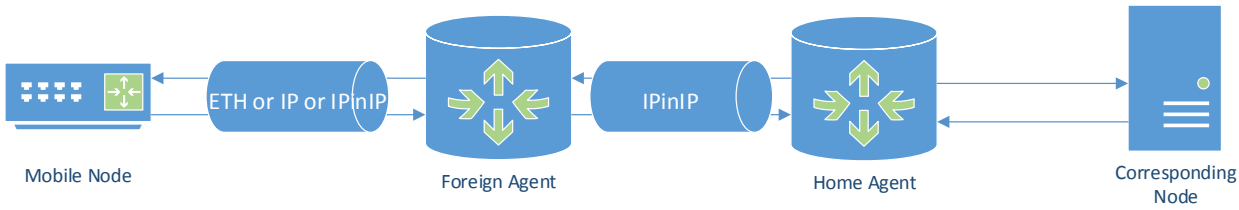

Figure 2-2 - Logical IPinIP Tunnels established between network devices.

There are several reasons listed under the RFC why IPinIP should be used, but the main reason at the time was to avoid the use of IP Options to have routers in an unknown network do routing based on source address, it is mentioned that because usually you don't have control over where the data is going through, it is not recommended and will possibly be ignored if you request a third party router to route based on source address. The mechanism used by this standard is as simple as putting an IP header in front of the original IP header (see Figure 2-3), although there will be several considerations in terms of security and routing of the actual packet. One of these considerations is the way that MTU is handled, because the added header may cause the packet to be fragmented if the payload is too big, a mechanism to set the MTU across the IPinIP tunnel has been put in place. If all the packets that go through the tunnel have the Don't Fragment bit set, then when the source of the packet receives the ICMP reply "Packet too big" (RFC 792 [8]) it will preemptively lower the MTU for the subsequent packets.

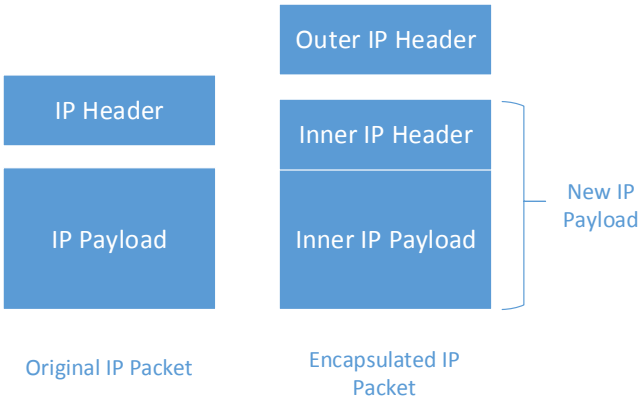

Figure 2-3 - IPinIP encapsulation.

One of the disadvantages of IPinIP is the fact that there is no Layer 4 header and so, if the outside network through which the traffic needs to go through to get to the Home Agent is actually the Internet, there is a very high probability the device will be using NAT to interface with the public network. As RFC 3519 in [9] describes, IPinIP has several issues with NAT but because the address translation depends on the use of ports, this makes one technology incompatible with the other one. It was partly because of this reason that the support for UDP in IP encapsulation was released in the aforementioned RFC. Using NAT not only causes an issue to the encapsulated IPinIP packets but also to the registration messages sent to the home agent; as it was previously mentioned, all the fields in the MIP registration request and MIP registration reply are authenticated, this includes the source and destination IPs. If the MN is using NAT its source IP will appear different once it arrives at the Home Agent and consequently will be discarded due to failing the verification step.

If UDP in IP is enabled and required, the Home Agent will now realize the MN is behind a NAT and will add the bindings matching the CCoA in the public network to the Home Address of the MN. All the communication must occur using a UDP port randomly assigned by the MN and UDP port 434 in the Home Agent. The IPinUDP encapsulated tunnel will be used only for user traffic and not for signaling, this will go outside the tunnel every time and as seen in Figure 2-4 the MIP header is sent in every single encapsulated packet. When using NAT, two aspects can be important for our environment, one issue is that that the packets should not be fragmented as only the first half of the packet will contain the port information necessary to maintain the address translation states, the other one is that NAT associations can change without the knowledge of the Mobile Node or the Home Agent and so there should be a mechanism in place that allows the re-establishment of the tunnel should the previous NAT information be invalid. The RFC proposes the use of ICMP Echo request/reply messages as keepalives in order to maintain the tunnel alive. The echo request messages will be sent with a given frequency and, as suggested from the RFC, despite not being required, the MN should receive an Echo reply in order to probe both ways of the NAT. If the MN doesn't receive a reply from the expected address, it will simply send a new registration message to the same Home Address it was previously using. As a final note that will be good to remember for this work is that even though NAT is being used, if there was an IPSec tunnel flowing from the MN to another destination, if the NAT changed, the IPSec tunnel would remain active without having to reestablish context, this is because the source of this

tunnel would be the MIP Home Address which will remain static for as long as the registration session stays alive in the Home Agent.

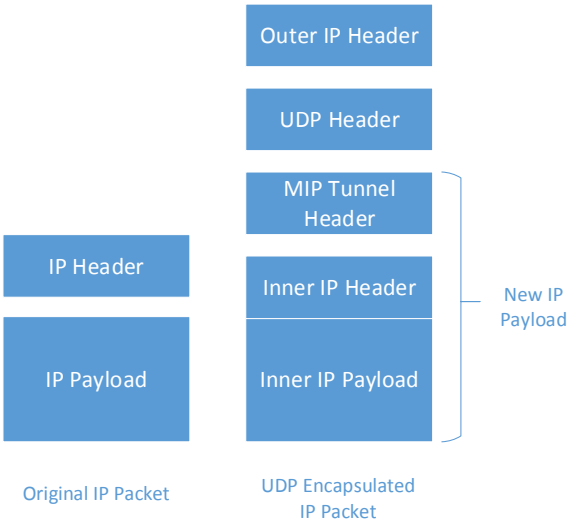

Figure 2-4 - IPinUDP Encapsulation.

2.1.2 MIP implementation in this work

For this thesis work, the MIP implementation used doesn't rely on ICMP advertisements but instead all the information needed is already configured in the Mobile Node and so only MIP registration messages are to be exchanged between the MN and HA, another important detail is that there is no Foreign Agent so all communication will be done using MN's CCoA through a IPinUDP tunnel to the HA, as Figure 2-5describes.

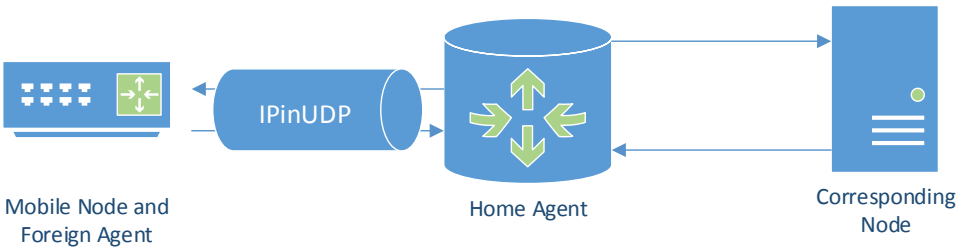

Figure 2-5 - Implementation of MIP used in this thesis.

2.1.3 Proxy Mobile IP (PMIP)

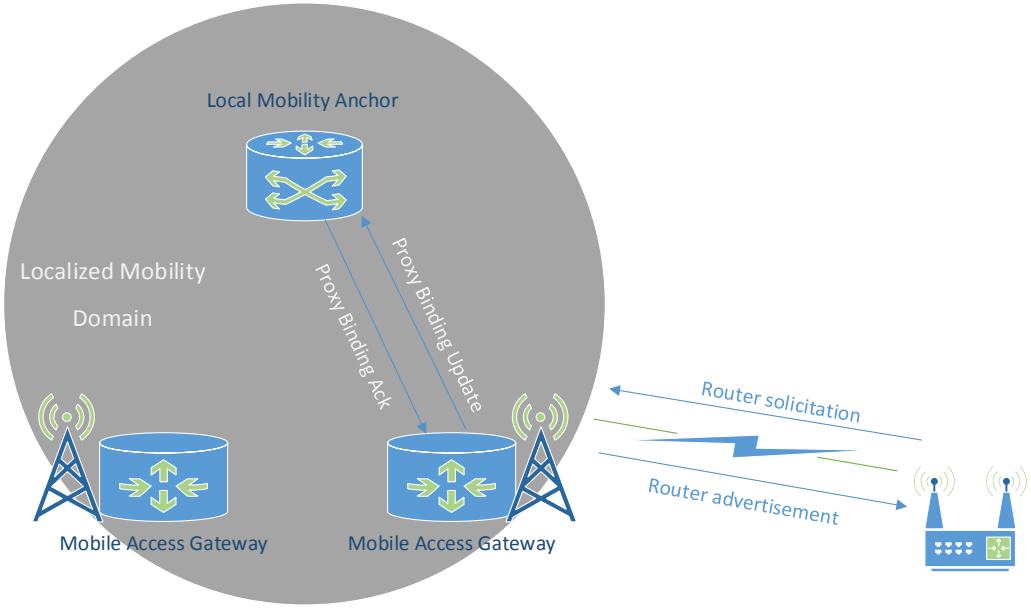

Figure 2-6 - Basic PMIPv6 message flow

Proxy Mobile IP version 6 was initially defined under RFC 5213 [10] and it will be described instead of Proxy Mobile IP version 4 as it was defined before and all the terminology was defined under the PMIPv6 RFC. It is possible to say that PIMPv6 is based on Mobile IPv6 (RFC 3775 [11]) and thus imports several of its concepts, such as the functionality of a home agent that stores all the information regarding the mobile nodes, in PMIP this task is offloaded mainly to the Local Mobility Anchor (LMA) which will have all the routes of mobile nodes inside its area of effect or the Localized Mobility Domain (LMD). Mobile Nodes are not to engage directly with the LMA but instead the first point of entry to the network; the access point, will contain a new PMIP entity, the Mobile Access Gateway (MAG). When a MN connects to a MAG, this one will relay the MN information to the LMA which will decide whether the terminal can make use of PMIP or not. Should the verification be positive, an entry is added in the LMA's routing table and a bidirectional tunnel between the MAG and the LMA is created so that the mobile node can communicate with its data services. Figure 2-6 describes the registration mechanism for PMIP.

The MN will initiate registration with its MAG through Neighbor Discovery for IPv6 (RFC 4861 [12]), MAG will send a Proxy Binding Update to the LMA and this one will send back a Proxy Binding Acknowledgment containing a network prefix that the MN will utilize as its outgoing interface. One aspect to notice is that the client does not require any software to support PMIP, only standard IPv6 functionality is required. Another detail is that there is a 3GPP specification (TS 29.061 [13]) that sets the rules and recommendations for PMIP in a mobile network, because of its functionality at access point level it can be used by operators to allow mobility to the end users.

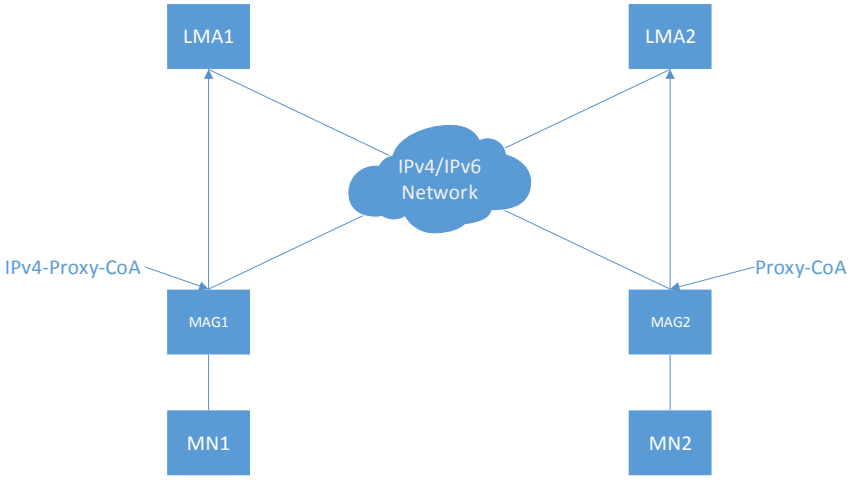

Figure 2-7 - PMIP with either IPv4 or IPv6. Source RFC 5844.

As IPv4 is being used mostly in every place in the network, it is also necessary for PMIP; whether is inside a 3GPP context or not, to function with IPv4 users or servers. It is suggested under RFC 5844 in [14], that any type of traffic should be able to make use of the local mobility anchors and so the whole network may function in either IPv4-only, IPv6-only or IPv4 and IPv6 modes. Looking at Figure 2-7 it's possible to see that either the LMAs or MAGs can serve as IPv4 or IPv6 endpoints. The document also suggests the use of tunnels to pass traffic in different types of networks, there could be IPv4 in IPv6 tunnels or vice versa, all with the purpose of allowing a full ecosystem of protocols to work with Proxy Mobile IP.

2.2 Examples of Mobility Technologies

According to the Cambridge Dictionary [15], Mobility can mean the action of physically moving around or could also mean the ability to have different services available to you regardless of where you move around. In practice, for there to be service mobility there needs to be access to the provider of said service and if we limit ourselves to internet services, obtaining access will depend on the availability of networks wherever the user is; effectively limiting the actual user's physical mobility if they constantly need service mobility.

2.2.1 Always Best Connected Paradigm

In a paper for the IEEE journal of wireless communications [16], Gustaffson et al described Always Best Connected (ABC) as the scenario where a user enjoys the best connection to the internet (or whatever services it is using) out of any of the alternate connections it has. It is suggested that a user can subscribe to an ABC service provider such that throughout the day the applications used will always traverse the most capable network to deal with that kind of traffic. This is interesting for this thesis work as ideally, our users should be connected to the best available network at all times; however, defining what would be the best for the user is something out of the scope of this project.

As an example of an Always Best Connected scenario would be if a user is checking their email or browsing the internet, the ABC provider may have the user switch to a network that has more bandwidth available. If later during the day the user requires to join a video

conference, the same ABC provider may the terminal device switch to a network with better response time and decent bandwidth.

There are several shortcomings with this paradigm because it will be up to the user or up to the type of application to decide what is Always Best Connected and this creates a very dynamic scenario where there are a lot of possibilities available for the ABC provider. As synthesis, ABC is the ideal that the user will always have the best network allocated to them according to their immediate needs.

2.2.2 Dynamic IP Allocation and Network Address Translation

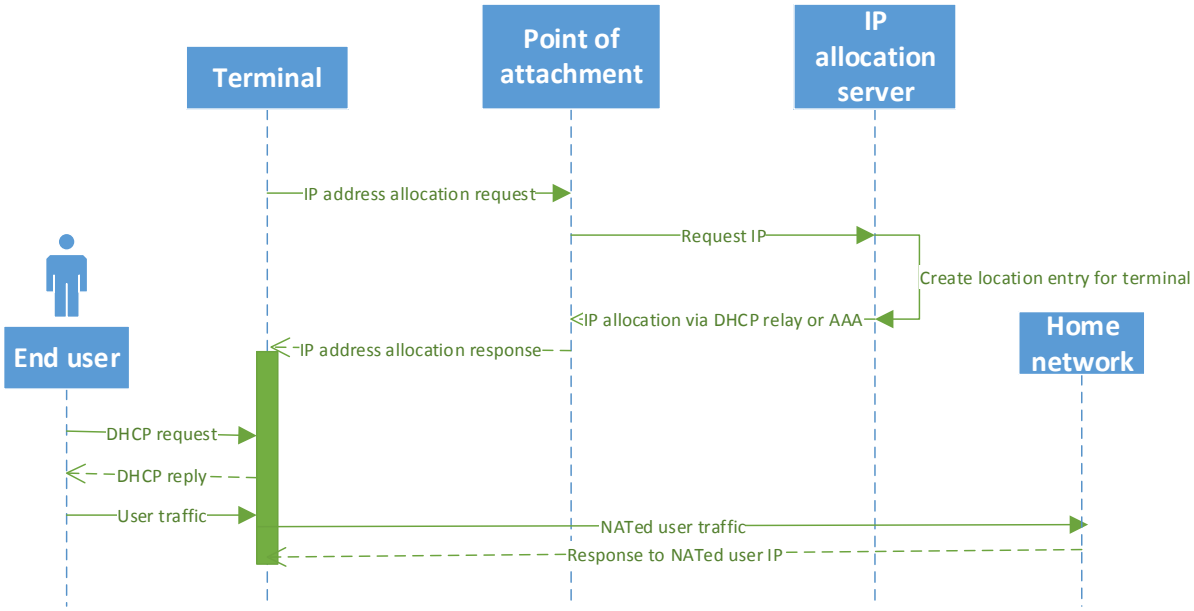

Figure 2-8 - Simple IP allocation and NAT process.

When a terminal device connects to an IP network, in order to receive or send any information, its interface will need an IP address. In the case of a cellphone, it is very likely that the IP is provided by the MNO, in LTE networks; as an example, UE (User Equipment) IPv4 address allocation is given by the through either DHCP or an AAA server [17]. This IP assignment is very important for the terminal device as this will be the origination of data that has to go through the MNO. The terminal's IP could be lost or changed due to different circumstances, the provider could refresh the IP every so often or perhaps the device simply lost its context to the MNO due to having lost all signal coverage. Roaming between MNOs typically results in the mobile device to have a new IP address; roaming could occur when you switch to a completely different network i.e, to a different country or, if the same user suddenly is outside its own providers' signal coverage the terminal device may proceed to roam as a guest in a second MNO's network [18], roaming across different providers could trigger a change of IPs in the mobile device's interface. Assigning IPs dynamically are usually done via the DHCP [19] although in some cases it may be different; such as via RADIUS [20], being able to respond to an IP address request message dynamically is important as it was noted there are many circumstances where a terminal may lose its IP. If

this device is serving as a default gateway to more than one user or application, the provider network would not be able to respond to any requests coming from outside addresses as it only has the information for the gateway's interface, Figure 2-8 describes a simple mechanism where the UE receives an DHCP or AAA allocated IP through a generic message and, immediately after the end user is able to make use of this address to source its IP packets via NAT. Using Network Address Translation (NAT) and Port Address Translation (PAT); described in RFC 3022 [21], allows to create a map between one or more network address to a single one and these days it is been used in most of the IP devices. NAPT could be applied at the terminal side or at the provider side and it creates a table such as the one found in Table 2-1 in order to be able to translate both outgoing and incoming requests. Using NAT and DHCP in tandem allows a user to be moving around without losing access to the internet services; if the mobile user is out of coverage area, the device will attempt to get a new IP from other providers in the zone and if there is a new IP assigned, any new traffic will be simply translated using NAT.

Table 2-1 - NAT table example.

Source IP	Source Port	Destination IP	Destination Port	NATed source IP	NATed source Port
10.1.100.10	63457	43.24.1.27	80	199.99.99.50	63457
10.1.111.50	13577	100.2.1.187	443	199.99.99.50	13577

The use of NAT and DHCP does not allow for seamless mobility by themselves as these are not mechanisms designed to execute or react to handovers but instead, if a new interface with better access to the internet was selected, any traffic flows that were tied to the old interface need to be updated with the new IP address, this means the user's applications would be disturbed while they re-establish new connections. Some applications depend more than other on their source IP; as an example any HTTP traffic is probably not going to be affected while any IPSec connections running in the terminal will need to be reestablished to recreate the context.

2.2.3 Routing Protocols

Making use of routing protocols requires at least two routing agents exchanging information about the networks they have available, this data will create a routing table on each of this routing agents such that each one of them will be able to forward packets to external destinations. Part of the information inside a routing table is the weight of the route to a given destination, this parameter aids in differentiating similar type of networks as it will cause the route with the highest weight to be chosen more often as the forwarding path. Taking this into account, we could take advantage of this weighting functionality and apply it in our environment.

For a routing protocol to be useful in this scenario, it needs to be able to change the active leg dynamically and this dynamic behavior will come from certain metrics that the protocol itself will need to acquire. For the sake of simplicity only the routing protocols that are currently available in the MNR; that is being used as terminal device, will be considered. Available protocols are given by the manufacturer in [22] and consists of: RIP, OSPF, EIGRP, BGP and

Cisco Performance Routing (PfR), Figure 2-9 describes the topology needed to implement a routing protocol, one routing agent being the mobile router and its complement would be a new device inside the DMZ (De-Militarized Zone). The protocol that we would need to choose needs to gives us the possibility weight forwarding paths not only on hop distance but also on dynamic information that can evaluate the link's quality. Based on this premise, we can say that RIP will not be suitable as it only provides hop distance information, OSPF only considers in its weight calculation how much bandwidth an interface has available [23]; however, this is a parameter that is not dynamic in Cisco's environment thus making this protocol unusable for us. BGP; as described in Cisco's article regarding large scale deployments in [24] obtains its weights based on static values and dynamically obtained from other routing protocols, the lack of dynamicity makes this unsuitable for our purposes, the EIGRP protocol provides more specific weighting parameters that can only captured from the data that the interface provides; this means the EIGRP protocol would judge the two routes by the characteristics of its local radio link and, the characteristics of its local 802.3 link towards the external modem, this sort of arrangement is not beneficial for our scenario as Ethernet links won't have the same physical constraints as a radio link and so it will be a biased weighting.

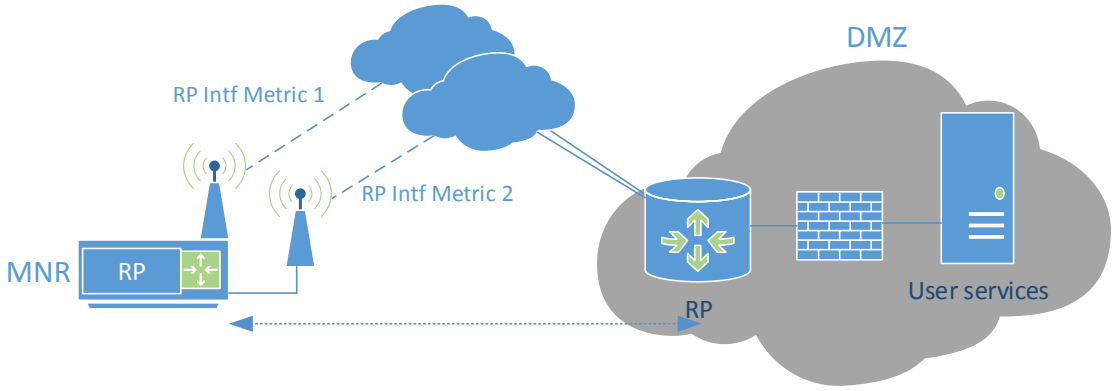

Figure 2-9 – Routing protocol architecture for the MNR.

Finally, Cisco's Performance Routing (PfR) makes a statement in [25] which vows to select the best available network; its policies are based on internal probes measuring items such as jitter, RTT and higher layer protocols responders. In reality this protocol provides a functionality exactly as is needed to achieve, in Figure 2-10 taken from the same document, the policies used for PfR are matched to several different objects and if a given threshold is reached an action is taken upon this traffic flow such as switching interfaces to a more reliable one. As is mentioned in [26], this protocol is meant for organizations to pass different traffic flows through alternate paths; however, we prefer standardized protocols that allow to expand solution to other vendors.

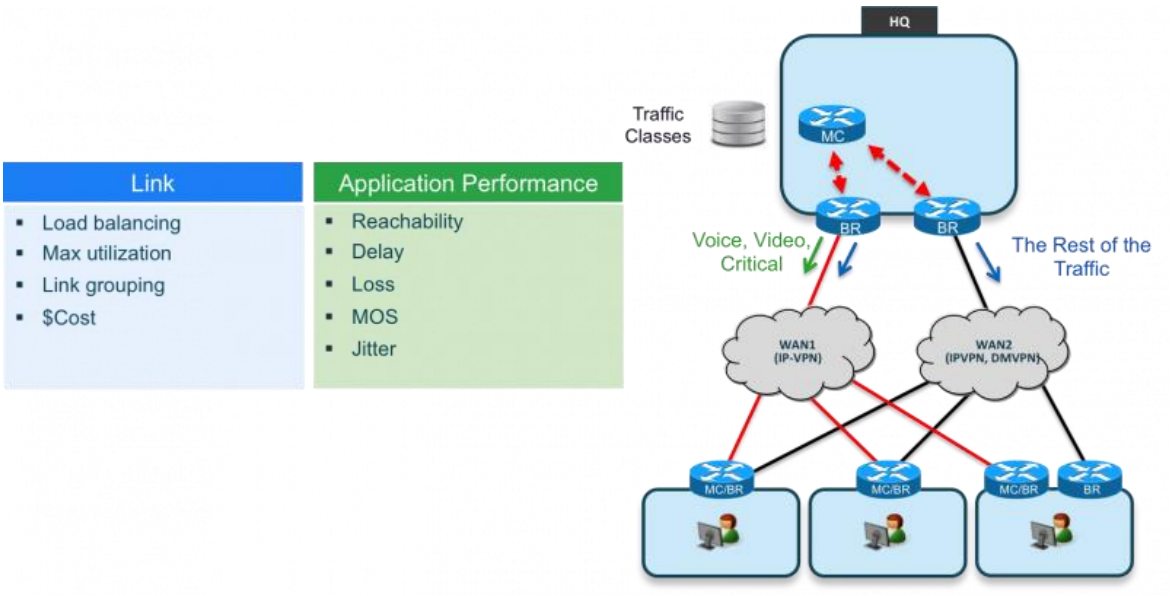

Figure 2-10 – Cisco's Performance Routing. Source: Cisco in [25].

2.2.4 Policy Based Routing (PBR)

The next topic to consider is Cisco's implementation of Policy Based Routing (PBR); which strips previously mentioned PfR from its core functionalities as described by Paquet et al in [27]. This mechanism will make it possible to take different measurements from within the client router itself and make a routing decision based on whatever has been configured inside the device. Among the characteristics that can be measured are round trip time, jitter, higher layer availability, interface status. Reading these metrics brings back memory of PfR, which can essentially use the same metrics mentioned previously. The main difference is that PBR is based on the premise that the client router has control over its own policies and can therefore, route without the need of an external server which provides the instructions.

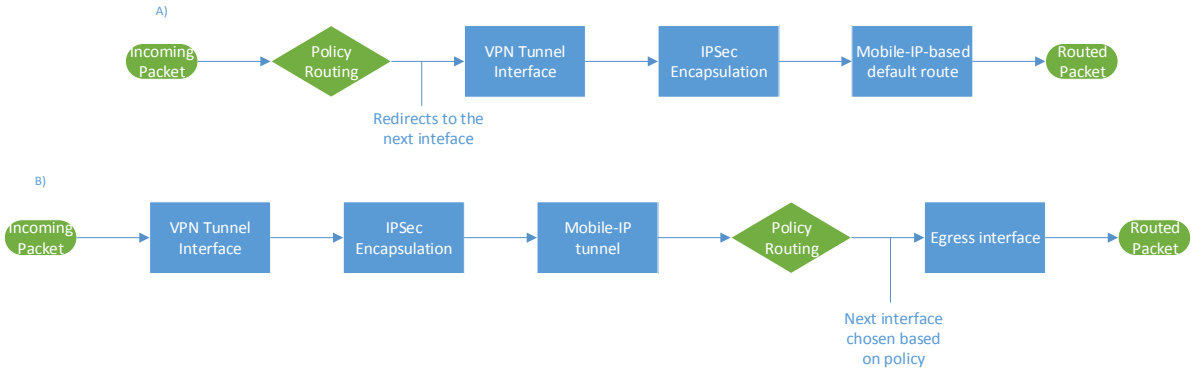

Figure 2-11 - A) Cisco's order of operations. B) Required order of operations.

One new matter at hand is the packet operation order within the router. Cisco has provided a basic order of operations in [28], the actual order is not readily accessible but the information in this document should suffice. Using Figure 2-11A as basis, PBR will be executed first before applying any encryption and before being routed, the flow would be as follows: the

packets are being generated by the MNR's user, once they are received at the router, if the policy is matched it will apply all the rules that were matched. Because PBR functions with the actual traffic and is not an out of band solution, this mechanism's next function must be to forward the policed packet to the VPN tunnel and proceed through the IPSec encryption and out of the MIP tunnel to be put into the MNO network. This creates a fundamental issue with PBR, because the probes will follow the same data path as the user plane data it will always probe the same outgoing interface which is in turn chosen by the Mobile IP protocol. Figure 2-11B shows what the router actually needs in order for PBR to be useful in this environment, what is image proposes is that the policing occurs at the last moment before the packets are sent out the router, this makes it possible for the probes to use different interfaces. This is essentially the benefit that PfR has over PBR; however, for this network topology neither of these mechanisms will provide the answer needed.

2.2.5 IEEE 802.21 (MIH)

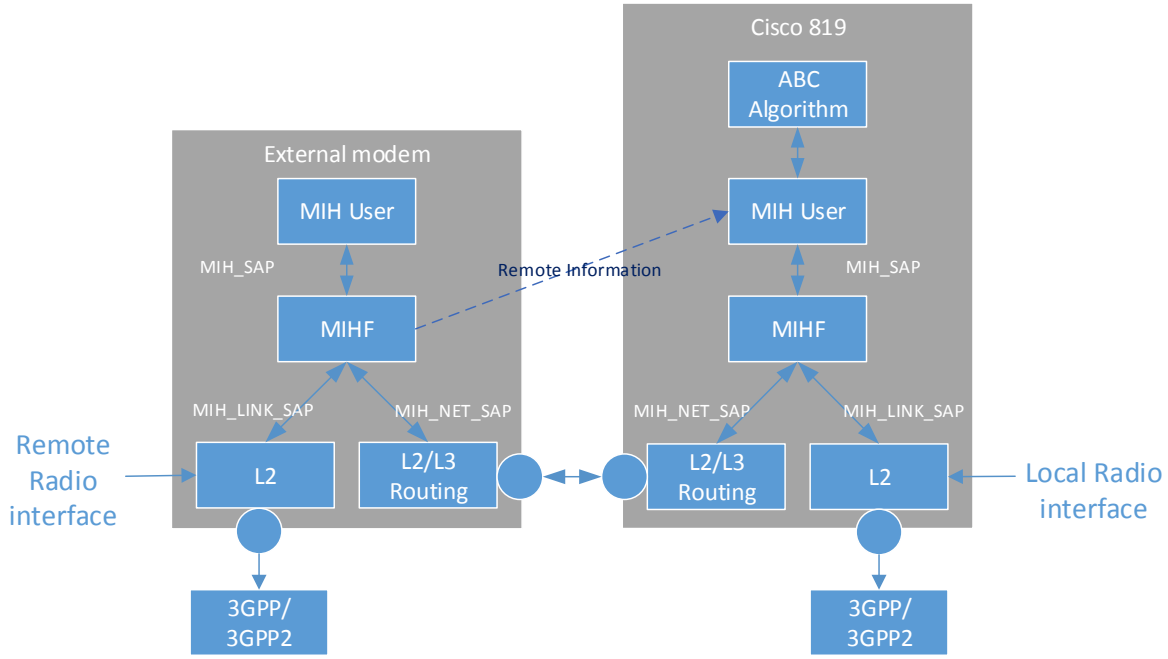

Figure 2-12 - Theoretical MIH objects needed in the current implementation.

When looking for an alternative to perform a vertical handover in a heterogeneous network environment, one of the alternatives that appears the most is IEEE's 802.21 Media Independent Handover framework [29]. MIH is a structure of interactions across abstraction layers to ease the handover procedure across different interfaces, because it is not a protocol but instead is supposed to function as part of a device's core functionalities it is supposed to interwork with any higher level IP protocol as Corujo et al explain in [30]. This thesis work requires from MIH is a mechanism to constantly probe and compare the available networks, and make a decision based on that. By itself, 802.21 doesn't provide a network selection algorithm to make a decision but it provides the tools to retrieve the information, store it and relay it to higher layer entities. This becomes clearer when analyzing Figure 2-12 which

depicts the elements that would be needed for the implementation of MIH in this environment. Following the process top to bottom, the MIH users will need to subscribe to interface events; because one of our outgoing links is located in an external device a remote MIH client is necessary, continuing along the network selection process, for the users to be able to subscribe to events, MICS creates the request and MIIS receives it and handles it. When MIIS receives the information it will need to pass that onto the MIH that was subscribed to that event and this user will then need to convey this data to whatever service needs it.

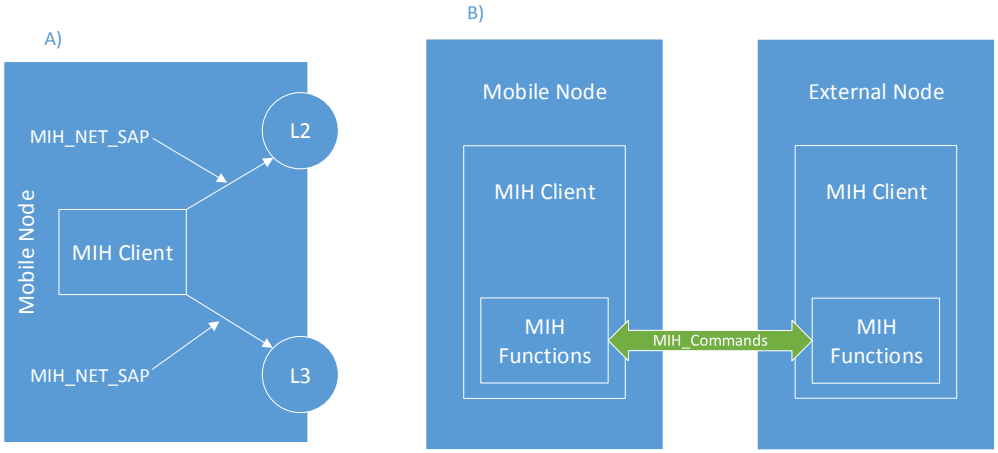

Figure 2-13 - A) Local communication to/from interfaces. B) Communication via remote MIH client.

For the purpose of this work, it is important to consider certain aspects of 802.21, the first of them is the fact that it has entities called Service Access Points (SAP) that deal with the communication across abstraction layers, the lowest of these layers is dealing with the physical interfaces and is handled by the MIH_LINK_SAP, this access point is supposed to create events forwarded to the Media Independent Event Service (MIES) or receive commands from the Media Independent Command Service (MICS). One more key aspect of MIH is the type of link events that are defined within 802.21's link state table, events such as Link_up.indication or Link_Parameters_Report.inidication are the sort of information our algorithm is looking for; the procedure is described in Figure 3.9, these events are the results of a command applied to the interface itself, in theory this means there must be some sort of interaction between the MIH Functions (MIHF) and the physical networks protocol via an addendum in their implementation; according to Taniuchi et al in [31], this was already in motion during the year 2009, this is true for 802.11 in 802.11u and, for 802.16 in 802.16g/m, according to IEEE's status report on 802.21 in [32], regarding 802.3 links, obtaining information directly from this type of interfaces is not yet possible as there are still no specific MIH_LINK_SAPs. In reality, a driver could be implemented at device level to relay the information from these networks (and also for 3GPP networks) to the MIHF. Figure 2-13 describes the MIH client communication methods, where it will use its MIH_NET_SAP to command or receive interface information or it will send or receive MIH_Commands from an external MIH agent.

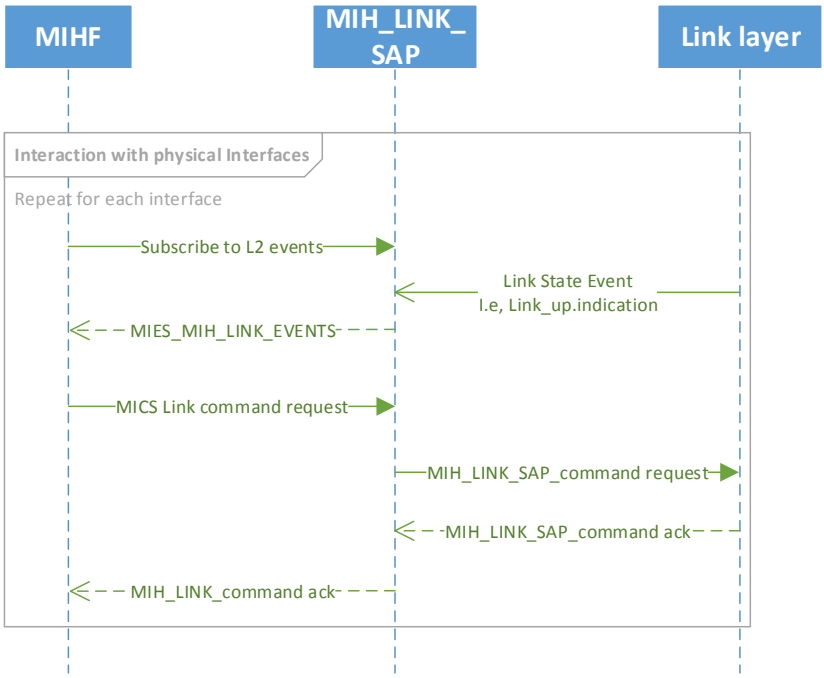

Figure 2-14 - MIH message flow.

There are several issues with this mechanism that refrain us from using it as part of the algorithm, the clearest option is the fact that there is no access to the external server thus the remote MIH client is out of the question. Consequently, retrieval of the remote information will be limited to the local interface facing the external modem which might work but there would need to be a correlation between the remote 3GPP/3GPP2 interface and the local 802.3 interface or at least there should be some information that can be inferred. It was already established that there is no 802.3_SAP available at the moment but it could still be a possibility; however, there still needs to be established if there is any correlation established in order to understand if there truly is a way in which this new SAP might be useful.

Comparing the remote radio interface to the local Ethernet one is well out of the scope of this work but then, what is important for the Network Selection algorithm is only to have information regarding all the interfaces that should be used for its election process, Figure 2-15 provides the updated MIH implementation for this thought experiment. The information that can be obtained on the specific Ethernet interface in the Cisco 819 is limited to buffer size, packet drops, data-rate interface errors and more; however, because the reliability of this link and the fact that there is a considerable difference in transmission speeds (1Gbps in the local interface against varying data rates for mobile wireless networks), there should be no impact whatsoever in the local interface regardless of what happens in the external modem.

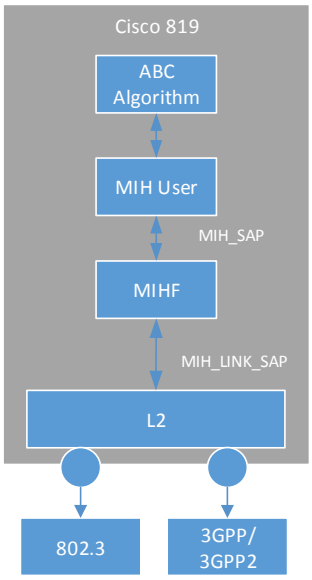

Figure 2-15 – New implementation of MIH without control of remote modem.

2.2.6 ANDSF

Now that features of MIH in the context of the current environment have been defined, other alternatives can be described and compared in order to retrieve the most important factors for a network selection framework. One of the additional procedures released as a standard is 3GPP's ANDSF; described in TS 24.312 [33]. This technology allows communication of enforcement of policies from an ANDSF server to the UE through a management object, this technology is meant to be employed by the owner of a mobile network in hopes of taking advantage of other non-3GPP transports, such as 802.11. This; nonetheless, means users of ANDSF are limited to a given provider's equipment and it is meant to be of an extra tool for the SP to control and manage how their users access the network. Implementations of this protocol have showed that it is feasible to event police different IP Flows, as Mustajärvi et al have shown in their test for the Future Internet Programme of TIVIT Finland in [34], ANDSF grants extends the possibilities a network provider has and can allow a given UE to connect to its system via non-3GGP sources. From this same project, it is clear this standard does not truly benefit our ABC algorithm as information of the links will go from the terminal to the SP and the handover choice will ultimately be in their hands.

2.2.7 Micromobility

When dealing with mobile networks, performing handovers between base stations should be done in such a way that the least amount of information is lost in the process. One way to make this happen is to apply the concept of micro-mobility which according to Campbell et al in [35], will allow the information to find its destination as efficiently as possible.

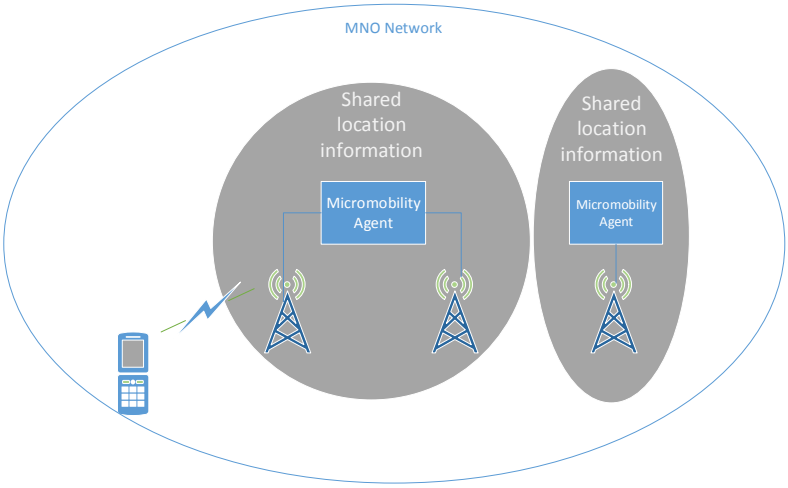

Figure 2-16 - Micromobility concept.

According to Campbell's study most of these algorithms allow the creation of generic entities between the terminals and the core network that have location information of users. In this micromobility network there can be different layers of information such that the micromobility agents (MMA) only need knowledge of an area in order to perform an efficient handover. In Figure 2-16 it's possible to that the MMAs will assist local base stations in performing the handover in an efficient manner. Not shown in the picture is the inherit capability of offloading information to different entities such that all MMAs could be connected one another or in a hierarchical fashion. There are different algorithms that allow core networks to benefit from micromobility such as Cellular IP [36], Hierarchical Mobile IP (RFC 5380 [37]) or IP^2 [38].

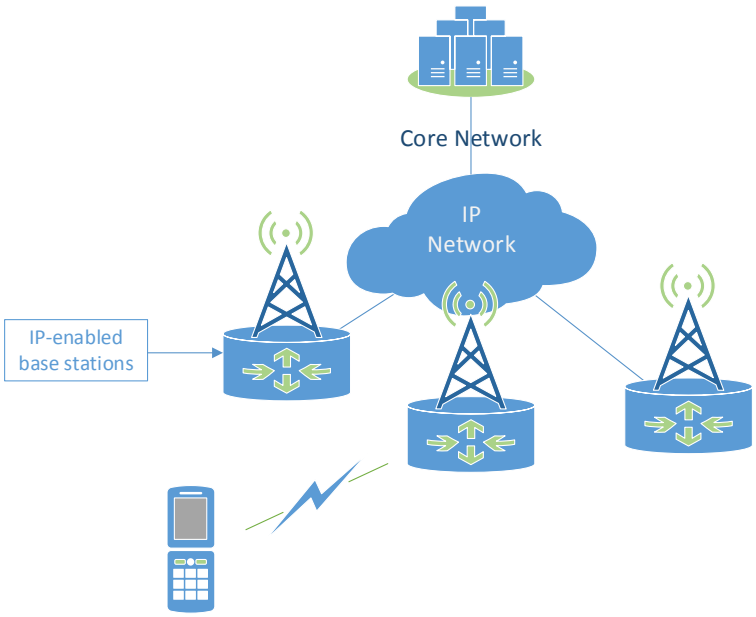

Figure 2-17 - IP-based IMT Network Platform.

IP^2 or IP-based IMT Network Platform proposed by Yumiba et al in [38], suggested having between the base stations and the core network an all-IP network that could take care of any handover decisions by simply allowing IP routing to take care of the process, this is shown in

Figure 2-17, where base stations will be included in the IP network in order to assist in routing decisions. The proposed IP Network allows for rapid traffic re-routing and vouches to minimize load in the network and handover delay. These micromobility alternatives; while proposing solutions for a handover problem, are only valid in the context of a service provider where information about the users is available and one has control over the networking path between the terminal and the services it is attempting to access. As such, these options are only included for the sake of completeness.

3 Design and Implementation of a Network Selection Algorithm

In this section we'll design a series of network selection of algorithms by investigating different vertical handover mechanisms and applying them into our design. The chapter will begin by introducing different concepts and interesting parameters to measure, then we'll go through a series of existing algorithms and analyze their applicability with our system. The next step is to separate our design into pieces that will be used to create the algorithms by distinguishing which protocols will be used and what part of the software and hardware are involved. One of the most important steps is to define which metrics are going to be measured, why and how. The final section elaborates a series of algorithms that take into consideration all prior research and that will be used in the implementation phase.

3.1 Study on network selection algorithms

As the first step to elaborate the algorithms we need to establish basic concepts and measurable parameters that will be interesting for us. At the same time, studying and analyzing a series of vertical handover algorithms will help understand what will work in future sections.

3.1.1 Vertical Handover

Vertical handover refers to the process where a networking device changes the access technology that is currently using to access its data services [39] [40] [41]. According to ITU's document on vertical handover considerations in [42], when a device changes its access technology it is likely that the IP at its point of attachment will be different and so any user data that is being sent out of the equipment will need to be reestablished and properly handled in the event of a vertical handover. To begin it will be important to understand which part of the hand over process will this study cover, in terms of the authors from [40] and [43] the basic vertical handover procedure order is divided in selecting the moment in which the handover process should begin; once the process has begun, what will be the actual process? And finally how to execute said process. It could be argued that initialization time is not necessarily part of the hand over process which is why [44], [41] and [45] split it as the data retrieval step, the decision algorithm and execution of the selection. In the next section of the study we will be focusing on the collection of network information and in the section afterwards we will go through the steps of implementing the algorithms and testing them.

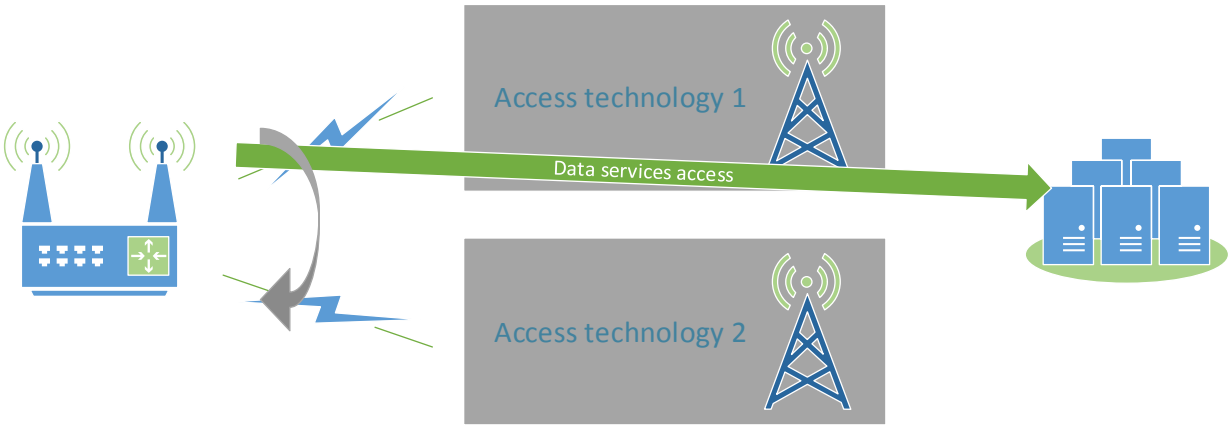

Figure 3-1 - Vertical handover overview.

3.1.2 Vertical Handover Schemes

The study will continue by analyzing different vertical handover mechanisms and network selection algorithms. There has been work put into categorizing VHO proposals and reports such as [40], [41], [43], [45]. It is clear that most of these investigations are based solely on wireless technologies and in most of the cases are tied to characterizing the radio interface in the terminal; however, by revising the output of these documents it should be possible to obtain an understanding of which are the common practices when dealing with Vertical Handover and Always Best Connected networks and apply some of the proposed theories and schemes to the project. Ahmed et al make a differentiation of instruments used to enable handover across wireless access technologies that will be useful as a stepping stone to proceed with the elaboration of the handover algorithm, see Figure 3-2. Using work from the aforementioned research papers should provide a good understanding of the available options.

These surveys provide key information about the researched papers and studies while categorizing them according to the authors' understanding and better judgement. In terms of selecting the actual mechanism and parameters, the categorization made by Ahmed et al fits the best this study as is the more in depth analysis from the studied papers, additions and exceptions will be made when comparing or adding information from other sources. Next we will begin the study of the different kinds of algorithms and the selection attribute.

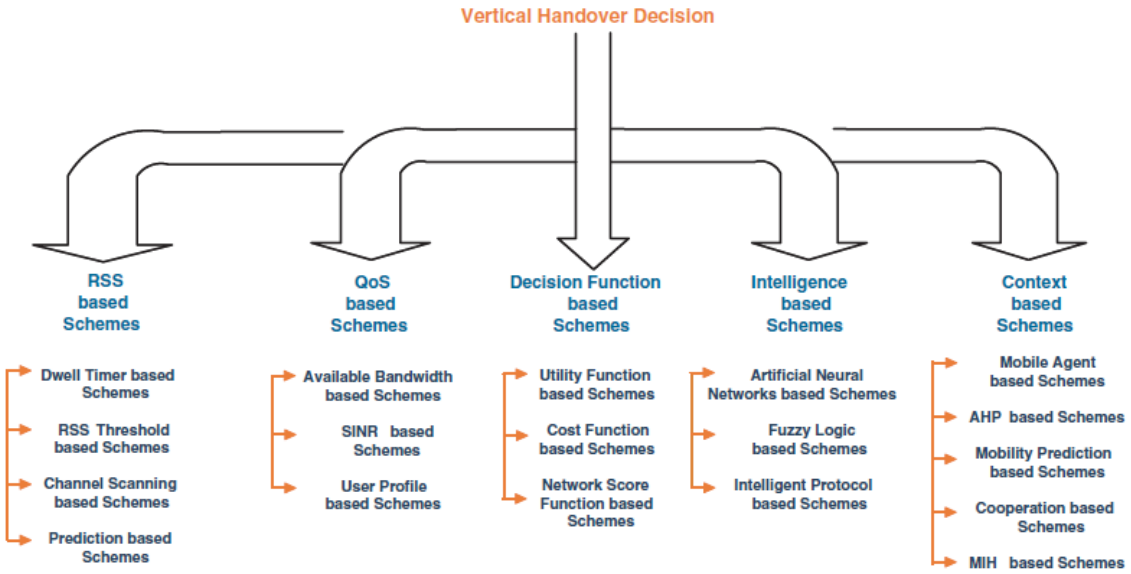

Figure 3-2 - Categorization of VHO schemes. Source Ahmed et al in [40].

In the work of Marquez-Barja et al in [41], several network traits are listed which are useful for network selection algorithms to make their decision, apart from Received signal strength, the CIR (Carrier interference ratio), BER (Bit error rate), SINR (Signal to interference and noise ratio), bandwidth offered, available bandwidth, network jitter, network overhead, security and, network coverage. From this same document we can also ignore the options that utilize information that our terminal can't use, these attributes are: the monetary cost of the network; because information is not disclosed to us nor it can the device obtain it, information regarding the physical location of the device; as the device has no means to generate this data and, battery consumption; because there is no limitation nor optimization needed in this area. We can correlate this information to [40]'s groups of algorithms and realize that all of RSS based schemes, the available bandwidth based schemes and, SINR based schemes will be out of the scope of the analysis. Context based schemes are; according to table 7 in the paper from Ahmed et al, optimal in different features such as reliability, less unnecessary handovers, handover latency, and more; however, as it can be seen in [46] and [47], these type of algorithms require the use of an external component to learn the context in which the specific terminal is located; hence these type of algorithms will also be excluded from the analysis. Table 3-1 provides a summary of the usability of the criteria that could be used as part of the algorithm, this information should provide an additional filter to verify if the surveyed schemes could be useful for our implementation.

Table 3-1 – Metrics that will be considered for the implementation of the HO algorithm

Metrics considered	Description
RTT	Round trip time from MNR
Packet loss	Percentage of packets failed to be delivered
Immediate throughput	Achievable data rate at a given point
User preferences	User selected priorities, such as a preferred type of application focus
Handover information	Feedback from HO process, i.e. HO success rate, HO delay

3.1.2.1 RSS-Based Schemes

VHO decision making algorithms can be divided according to the criteria they are to select the best network, there are one-parameter algorithm as well multiple-parameter algorithms, the simplest ones ([40], [43], [44], [41]) are the ones that require a single characteristic from the network to make such choice; one of the most available algorithm options are the ones based on RSS (Yan et al, Table 3 [44]) and because of its popularity and relative uniqueness due to being inherently tied to the physical interface of a wireless modem, it was given its own category. This type of mechanisms analyze aspects such as Signal strength, cell signal overlapping or channel availability, all of which it is a must to obtain from the network itself for this information, algorithms such as the one suggested by Lee et al in [48] require from the network the signal strength and induct the available bandwidth from the selected type of access (i.e., up to 54 Mbps for 802.11g). Applications that rely so heavily in data obtained from the wireless access network itself will suffer in its applicability if applied to our abstract black-box interface concept, which is why such attributes will be overlooked.

3.1.2.2 Single-Attribute QoS Schemes

In general ([40], [41]), user profile schemes turn to the operator of the terminal to decide what parameters will be used to switch from one network to the other and some of them ([49], [50]) will even have an additional tools to aid the user in the selection of the best available network; however, one of the advantages in these type of algorithms is also a limitation for our environment, as Cavagna et al show in [50], with the help of user interaction it is possible to optimize quality of experience exactly how the user needs it, taking out the assumptions any implemented algorithms could make from the operation of the equipment, Cavagna et al explain how an algorithm that tries to be always Best Connected, may not always feel the best for the actual user; an example that could very well be applied in our case is the IPSec tunnel having to be re-established every time a handover occurs, even if it is going to connect to a better network, if the user is not really going to need the extra quality, it could probably cause impose an inconvenience. In this paper, a user profile engine is proposed, that will form part of the input in the network selection process. Kassar et al in [51] propose a an architectural similar strategy where user preferences are also taken into account; however, in this work the operator of the terminal provides an ordered list of network qualities priorities, as an example a list could look like this: high throughput, low latency, low cost. With this information the network selection process could make several runs depending on which interfaces are available and if they are, what metrics are obtained from them.

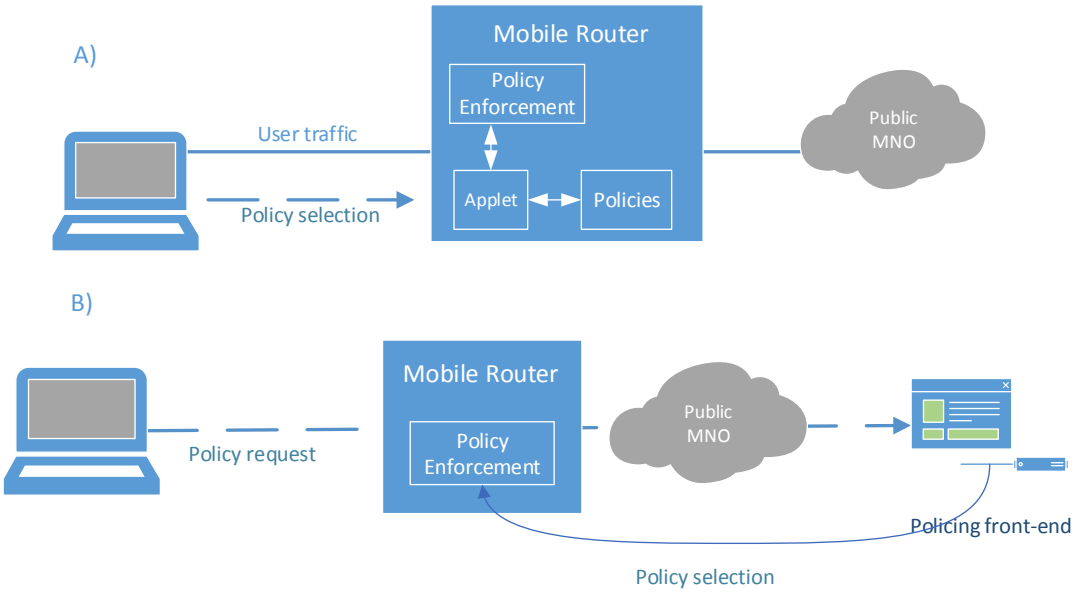

Figure 3-3 – A) Policy selection via local applet. B) Policy selection via external server.

One of the limitations of this project is that access to the MNR is forbidden from the users as a design choice and, creating a portal in a remote server to allow user access control over the device is already not possible due to the reasons explained in Section I. Figure 3-3A and B aid describing the limitations in user defined profiles schemes applied to our setting. Without the possibility to implement such type of input into the hand over selection process, the benefit of these scheme is lost as the procedure that will select the new network won't be compared to the users expectative of the network. In synthesis QoS-based schemes are only as useful as the attribute they use to make the network selection, this means that if it is a Link-layer metric it probably won't be useful for our environment; however, if we were to use Round Trip Time or Immediate Throughput as the sole parameter for network selection, it could be used as one of the most basic algorithms, where data will be collected on this one metric and a decision will be made according to which network has the best value. One learning that can be taken from the user-profile based selection mechanism is the fact that the network selection may not be left to the user alone but instead, user input was used to alter the implemented network selection algorithm in a higher layer of the handover process; Figure 3-4 exemplifies the mechanism, this is a tool that could be applied not as a user but instead as owners of the MNR, by setting our own static preferences we could earn a degree of flexibility but not gain as much in quality of experience for the user, this type of algorithm will be reminded to us in when studying the following schemes. Next in order, the study will continue with decision function (DF) based schemes; which provide multi attribute algorithms for network selection, both user and network oriented, these type of mechanisms provide increased flexibility and automation but as mentioned in table 7 from [40], it could introduce an impactful ping pong effect or produce several handover failures.

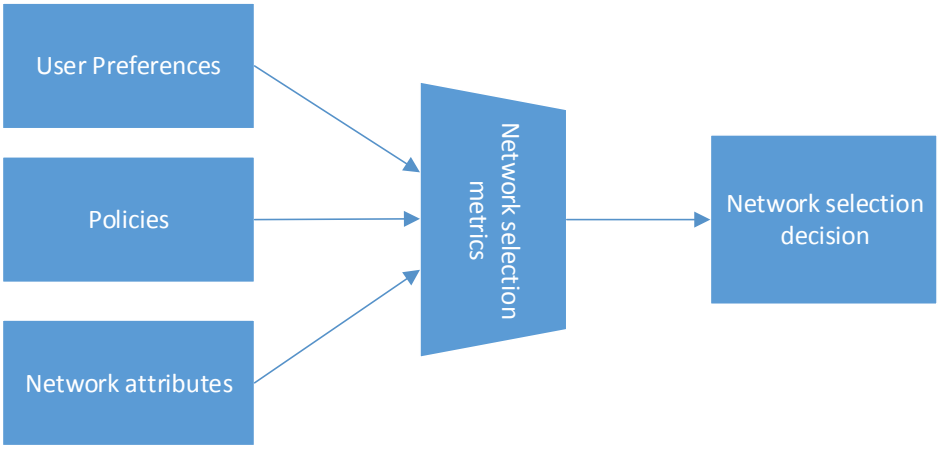

Figure 3-4 - User preferences influence in the algorithm.

3.1.2.3 Multi-Attribute-Based Schemes

In the scope of DF-based schemes it is possible to find network-cost-based algorithms and utility-based algorithms in the main idea is that for each access network available, there will be a set of metrics taken from it, the data will be processed and finally there will be a mechanism that will make the decision of which network to use. Ahmed et al provides a description and explanation of Utility based schemes, it is mentioned in order to select the best utility function it is necessary to know what type of user will benefit of the network selection mechanism; it could be a user trying to save as much time/money as possible or a user who doesn't mind how much time or money will they spend. This type of models will contribute in granting a higher quality of experience for the operator of the equipment; however, it is reliant on detailed network information to produce the best result and also needs to consider the users' input to decide what the best utility function is thus this really doesn't provide much usability in our setup as there will be no interaction with the users and, most of the network information is unavailable to us.

In the work of Mohamed et al [52] they mention how Multi Attribute Decision Making (MADM) algorithms provide increased flexibility when selecting a network across many because one can assign different weights to the criteria allowing or limiting the dynamicity of the mechanism. Kassar et al in [51] list the some of the most prevalent MADM tools: Simple Additive Weighting (SAW), Analytic Hierarchy Process (AHP), Grey Relational Analysis (GRA) and, Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). This different mechanism attempt to solve the same issue and will do so by having different degrees of complexity, automation and accuracy, in this study we will evaluate popular released MADM works and verify if it could be applicable to the scenario at hand. It is important to remember that while all these papers are focused on wireless networks our main concern is if these same mechanisms could be applied to a generic-type of interface to make the handover decision and, because the user-profile based schemes were a no-go, the list of available metrics is limited through the following:

RTT: the system must send a packet, receive a response and be able to obtain the value.

Packet Loss: the network will be probed by sending a pre-determined amount of packets and obtain the % of actual received packets in the destination.
Immediate throughput: the interface should be able to provide the amount of bytes transmitted and received, or there should be a mechanism in place to probe the network and obtain the resulting data rate.
Handover information: Handover procedure-related information may be logged and may be used as input for the algorithm.

We will then proceed to break out some of the MADM mechanisms and conclude from this if the scope of the studied works can be applied in our environment, the way that this will be evaluated will be by selecting some surveyed algorithms until we are able to obtain the space in which each one of the multi-attribute algorithm types can be useful for us. The study will begin with an Analytic Hierarchy Process algorithm for which the authors in [51] divide it into three sections, first there will be different decision levels in which different criteria will be analyzed, then within the same level the collected data needs to be processed and lastly get the resulting weight of each level in order to select the best result. Qingyang et al make a case for AHP and GRA in [53], the authors propose that utilizing the AHP framework, the actual network selection will be done by utilizing a Grey Relational Coefficient (GRC). The GRC is a normalized function of the results from the different QoS levels in their proposed "Data Processing" step, which is the authors' way of calling the AHP mechanism. In this work several levels of criteria are analyzed and treated based on actual environmental data and actual user requirements, Figure 3-5 attempts to apply Song's proposed algorithm to our environment and explain the different steps involved in it and because it is not taking into consideration past handover history, only the RTT, Packet Loss (PL) and Immediate Throughput (Th) QoS values will be taken into account when gathering data.

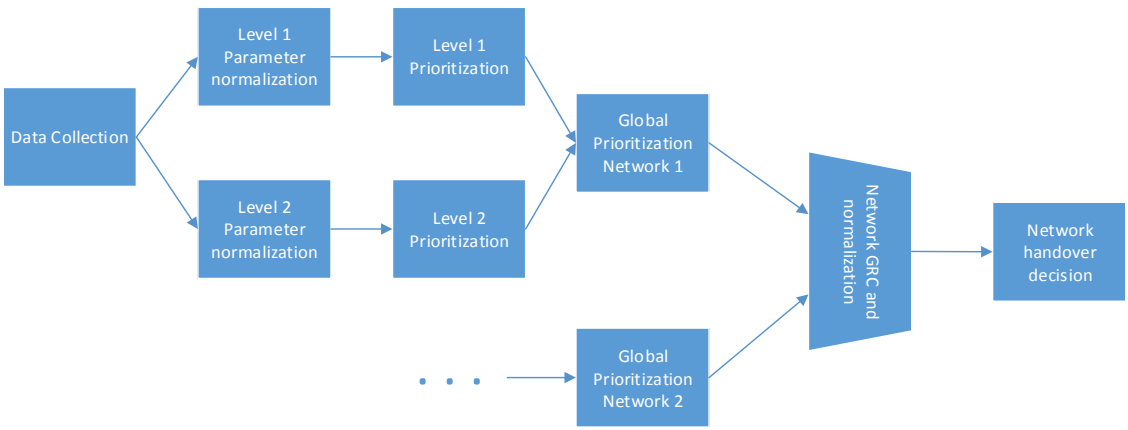

Figure 3-5 - AHP / GRA mechanism based on Song et al [11].

In this example, every step needs to be done for each access network available except for the aggregation GRC calculation step and the actual decision-making step. The Data Collection stage will feed the parameter normalization process the values of RTT, PL and Th. What makes this an AHP-type algorithm is the fact that we would want to make the network

selection based on immediate throughput but, we also want to qualify this criteria based on actual packet round trip time and loss percentage; which is what the Level 1 and Level 2 prioritization steps will produce. In the Global prioritization phase there will be the product of the output from the previous steps, creating a unique set of normalized Level1/Level2 values. This global set will then be used to create a GRC for each access interface, where the higher the value, the better. Once GRCs are obtained a network decision can be made and handover may proceed. As conclusion, architecturally this framework can be applied into our environment, AHP and GRA are generic enough so it allows for any type of interface in principle; however, one key aspect can be drawn out of the mechanism at hand and that is AHP's biggest benefit is allowing the division of the attribute analysis into stages and obtaining the relationship to the rest of metrics, in tables 4 and 5 from Qingyang et al, the authors established the relationship between every parameter and that allows for the optimal result when utilizing grey relational coefficient. This relationships inherently mean that the metrics should be somehow linked to each other but unfortunately that is something that can't be obtained in our environment. The available network data that can be obtain from of RTT, PL and Th are not related to each other in the sense that the round trip time or loss of packets information from the actual user load (or immediate throughput) can't be taken from the user traffic but instead, needs to be taken separately. Consequently, all of these parameters are qualifiers of the immediate network information not to the actual user experience, furthermore it can be said that the [RTT, PL] set can't be used to describe [Th] and vice versa. Because there really is no need to increase the complexity by separating non-related properties into different processing stages, a simpler mechanism to make a network selection decision would be the Simple Additive Weighting method.

The SAW procedure is one of the simpler there are because all it is meant to do is select the interface to be used based on the product of a given criteria with its weight. Nguyen et al in [54] provide a summarized view of SAW in (3.1), where the network attribute x_{ij} is multiplied by its weight w_j. The highest interface's product will then be selected for the HO decision. A different kind of weighted mechanism is the Weighted Products approach, its equation (3.2) makes it clear that while the ultimately is the same kind of process, it allows for any combination of measurement units to be used in the equation, as opposed to the SAW model where there needs to be a single type of unit.

$$A^*_{SAW} = \max_i \sum_{j=1}^{m} x_{ij} \times w_j \qquad (3.1)$$

$$A^*_{WP} = \max_i \prod_{j=1}^{m} {X_{ij}}^{w_j} \qquad (3.2)$$

These two schemes; while being simple in their way of working, provide a sturdy enough solution for many kinds of networks. The results from [54] show that, while compared to TOPSIS algorithm; which will be analyzed up next, these simple mechanisms provided a similar response in many of the cases. One of the added benefits is that; much like GRA, SAW and WP could be used in conjunction with other tools to make a more accurate selection algorithm. In general, SAW and WP are not dependent on any kind of network or attribute therefore there is no impediment in utilizing these tools in our environment, we would only need to normalize the data from any of the attributes at our disposal to be able to make use of the SAW model. For the sake of comparison it will be good to analyze the

Technique for Order Preference by Similarity to Ideal Solution algorithm which; according to Nyguen et al, is one of the most popular interface selection mechanism used.

Bakmaz et al describe in their article [55] how the TOPSIS method provides a tool for ranking different networks sequentially based on network attributes that will have different weights for the decision process. Information provided in [55], [56] and, [57] suggest that for TOPSIS to be as efficient as possible Available Bandwidth, QoS Level, Security and Monetary Cost ought to be used as criteria for the algorithm; however, this framework is not limited by the type of parameters it can use therefore we may proceed with this analysis. In order to make a network selection decision TOPSIS requires that all the data is normalized and every network characteristic must have a weight associated to it by the actual user of the equipment, or as is suggested in [55] using the entropy method to relate a given parameter to the other ones. The result will be a matrix as in Table 3-2 based on the work of Bakmaz et al ([55]) in which the data will need to be normalized, subsequently there will need to be a matrix of the weighted network parameters. As in the SAW/WP analysis the parameters used will be RTT, PL and Th. With this information TOPSIS will proceed to retrieve the best solutions and the worst solutions out of the weighted attributed so it can then obtain the Euclid alternative distance which will characterize a given network i's attribute with respect to the best (Di+) and worst (Di-) solutions in (3.3) and (3.4).

Table 3-2 – Matrixes of TOPSIS parameter information.

Normalized matrix			
	RTT	PL	Th
Network 1	x_{11}	x_{12}	x_{13}
Network i	x_{i1}	x_{i2}	x_{i3}
Network n	x_{n1}	x_{n2}	x_{n3}
Weight j	W_1	W_2	W_3
Weighted matrix			
Network 1	$W_1 * x_{11}$	$W_2 * x_{12}$	$W_3 * x_{13}$
Network 2	$W_1 * x_{21}$	$W_2 * x_{22}$	$W_3 * x_{23}$

$$D_i^+ = \sqrt{\sum_{j=1}^{3}\big((Network\ i\ parameter\ j) - (Best\ solution\ i\ parameter\ j)\big)^2} \quad (3.3)$$

$$D_i^- = \sqrt{\sum_{j=1}^{3}\big((Network\ i\ parameter\ j) - (Worst\ solution\ i\ parameter\ j)\big)^2} \quad (3.4)$$

$$RC_i = \frac{D_i^-}{D_i^- + D_i^+}, RC_i \in (0,1). \quad (3.5)$$

Because in our environment there are only two networks, the weighted matrix in Table 3-2 will consist of two rows which will feed the data to the equations above in order to obtain the distances to the best and possible solutions. These results will then be used to calculate the relative closeness (RCi) (4.5) which as research paper indicates, will provide value that will be used in the network selection decision; simply put, the higher the relative closeness to the best solution, the better is the network. There is; nevertheless, one aspect found in these papers aforementioned research articles at the moment of the algorithm's implementation because these authors are filtering any networks that do not fulfill a pre-determined set of

RAN link conditions so any access networks with very poor quality will not enter the TOPSIS handover process. It is reasoned that the motive behind this is that every network that is to be taken into account, will affect the actual process, even if its quality is extremely low. As an example, given 3 networks with available bandwidth (b), network 3 is suffering from very poor link quality so the respective bandwidth values are: 10 mb/s, 200 kb/s and 10 kb/s. For b and any other attribute taken into account, there will be new values from network 3 that may alter the results had it not been considered since the beginning. Overall, this initial filter will make it so that at least processing time is saved and at most it will keep the mechanism from making any biased decision. Figure 3-6 shows how a network decision algorithm based on TOPSIS would look like in our current environment. Filtering the data might be interesting for our algorithm; however, because we are lacking RAN-based information it will be needed to rely on either RTT or PL parameters as immediate throughput is the best alternative available to make a selection in the current environment. Furthermore, work in [55] has been done in include a hysteresis (h) margin to reduce the amount of false handovers while leaving the rest of the process intact. This extra value will provide a level of flexibility to the algorithm wherein despite the new network being better than the currently active one, if it is only marginally better for the user there is no relevant gain from handing over to this new interface.

In the AHP/GRA section, it was mentioned that the parameters of RTT and PL are not directly related to the immediate throughput but instead these must be obtained in a separate test, in this case the round trip time probe can be the same as the packet loss probe and so one can say these tests serve to qualify the network at the same moment in time this means there could be value added to using these two metrics as filters to verify which networks will be then processed through the TOPSIS algorithm. As a summary, this multi-attribute method provides a way to compare different network characteristics, calculate their distance to the ideal solutions and rank the networks based on the one that provided the closest distances to the best available offers. This scheme allows to be used in a generic-type of interface; however, as it was shown it is preferably to have a mechanism in place to select which networks will participate in the network decision algorithm so as to not interfere and bias the ranking of the contributors. An important aspect to take into consideration when using this tool is that is that networks will be equated with themselves and an over-performed will be chosen to be the active one among all. To compare these networks to a threshold or a given point in the performance of the network might not be trivial and the studies analyzed do not provide an answer to this, thus this question will remain open and will be put to test when analyzing implementation decisions.

With TOPSIS, the DF-Based schemes have been studied with really interesting results, a summary of this section including user-profile schemes, SAW, WP, AHP, GRA and TOPSIS, is provided in Table 3-3. SAW, WP and TOPSIS are methods that can be used on their own to make a network decision, as seen in [56] TOPSIS can also be further improved with some filtering done before it can process any data. GRA; much like TOPSIS, will provide a value that can be used to rank networks but does not consider how far are the parameters from the worst case.

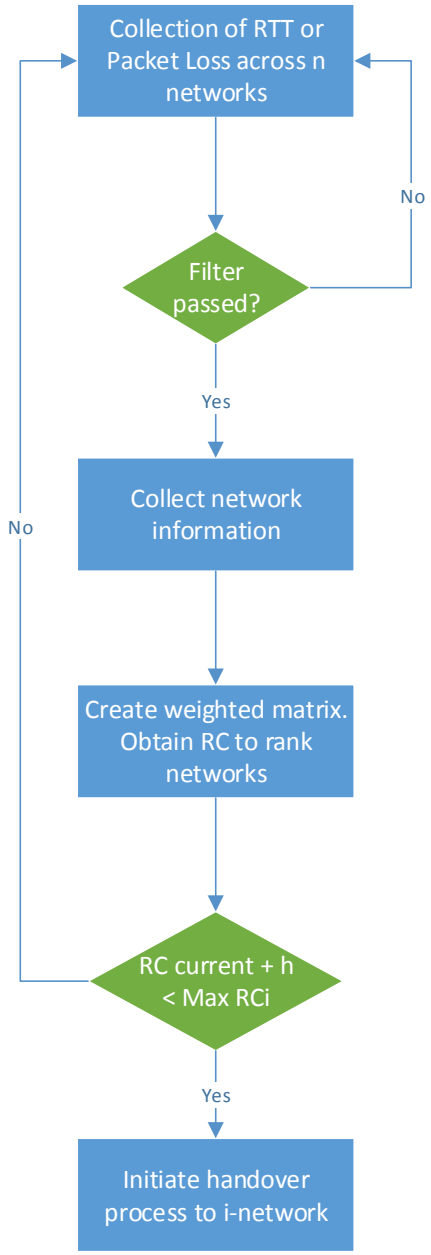

Figure 3-6 - TOPSIS based Network Selection algorithm. Based on [13].

GRA, AHP and User profile-based have been ruled from being further studied, in the first two cases the scope in which they can be applied greatly limits their usability therefore it will take much work for a not so high benefit, as for schemes making use of user profiles, we have denoted how this meets an architectural limit in our environment as the user is restricted from interacting with the terminal. In the next sections we will study Network Intelligence (NI) based schemes and Context based schemes. Ahmed et al in [40] explain how NI schemes use more complex functions and feedback loops to solve issues where a more granular control over the traffic flow is needed, such as real-time data and the issue of missing packets when performing a handover.

Table 3-3 – Comparison of the studied mechanism in the current section.

	Interface-type agnostic?	Dependent on a specific network attribute?	Usable in our environment?	Reason
QoS-based schemes	Depends on metric	No	Yes, depending on metric	QoS-based schemes can analyze one single attribute, depending on which one is used, it is available to us.
User-profile based schemes	Yes	No	No	End-users have no access to terminals
Utility function based schemes	Yes	No	No	Is best applied when there is user interaction and more information about the network
SAW/WP mechanisms	Yes	No	Yes	May be used as tools to complement the algorithm
AHP framework	Yes	No	No	Will not provide significant advantage due to limited amount of metrics available
GRA algorithm	Yes	No	No	Overly complex for our limited resources
TOPSIS algorithm	Yes	No	Yes	May prove to be useful as a tool

3.1.2.4 Network Intelligence-Based Schemes

NI-based algorithms provide a tool to make much more accurate and complex decisions, Yan et al in [44] mention how using fuzzy logic (FL) or combinational logic (CL) allows an increased amount of inputs to participate in the network selection process, using fuzzy logic even accounts for erroneous or imprecise data and either corrects it or ignores it. In the table 1 from Kassar et al, they explain how important using different attributes is for FL type of algorithms but not so much for Neural Networks (NN) however, because of its underlying topology NN schemes will be far more complex to implement than FL-type. Many implementation of NNs for handover decisions require network-side information or rely the decision to the network so as to save processing time [58] or require specific network information such as RSS or Terminal velocity ([59], [60]), the same could be said of Fuzzy Logic based algorithms where their strong points come to light when they have plenty of up to date data. Ahmed et al continue to make a case of FL-based schemes by describing popular algorithms in this category; all of them however, make use of specific network information, terminal information and/or user interaction. Along with FL and NN methods, intelligent protocols such as SCTP and SIP that will account for any interface changes and will maintain their traffic flows active regardless of where are the packets supposed to be going though. A synthesis table with the works analyzed in the authors' work can be found in table 5 from [40] but; while providing superior network selection capabilities, the implementation complexity and the amount of information need prevent us from making use of NI-based schemes.

3.1.2.5 Context awareness based scheme

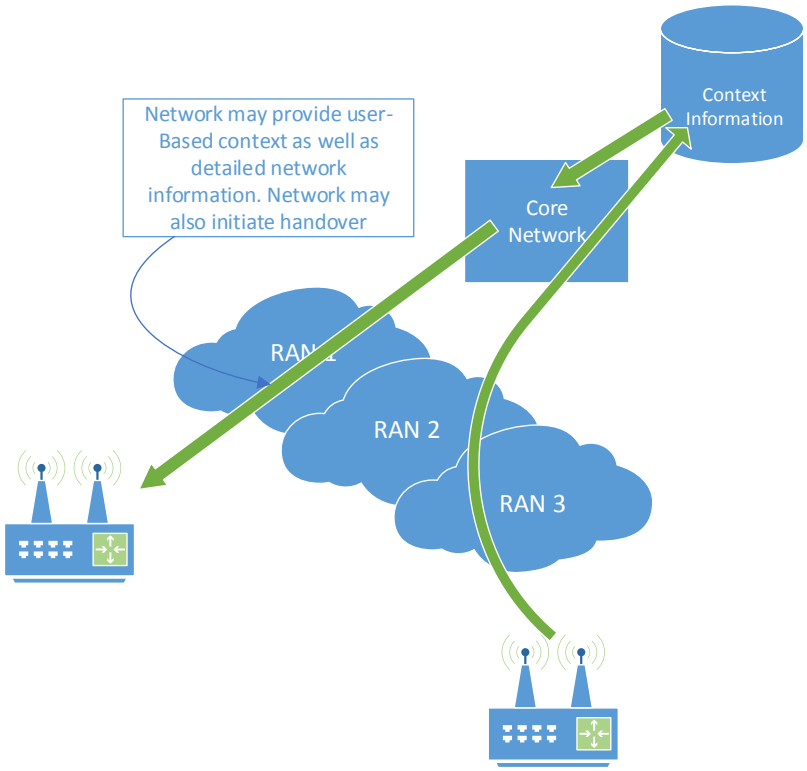

Figure 3-7 - General context based scheme's topology.

Following in the study list are the context-based schemes which meet us with plenty of the same requirements as NI-based schemes, in [40] there is a summary of the most popular type of algorithms in this area. It is true that because there will be a big amount of knowledge of the network, the algorithms will provide an advanced handover mechanism with greatly improved QoE and optimized timing such is the case of Zafeiris et al in [61] where the authors introduce a Multi Access Provider (MAP) which obtains information from the roaming agreements between different Network providers and is able to provide options for the terminals at the time of executing a handover. In this example the network decision algorithm will take into consideration values such as type of communication (duplex, half-duplex, multicast, unicast), type of terminating network, accessible core network types, access interfaces and cost, all of these attributes will then be used in connection to network load and terminal information in order to let the MAP make an informed decision of where its users are and will be. Many of other context aware such as [62] and [63] rely on the network to provide context information which allows for a increased understanding of the surroundings and ensures an accurate handover decision (as seen in Figure 3-7); nevertheless, this come with a price our system can't pay. It won't be possible to provide any type of context as the only information available is for router in question and there can't be any more protocols in place since there won't be any responder outside of the terminal. Making use of context-based algorithms in a generic-type interface is a good topic of study as the articles provided in the table previously mentioned all make use of wireless network technologies.

In synthesis, we have managed to draw out even more limitations in our environment when put against the many kinds of handover mechanisms that were studied. It was noted that RSS

the most popular attribute to use as part of the network selection process; either by using it by its own (as in the described RSS-based schemes) or in many different algorithms as part as filters (as mentioned by Yan et al). It was also analyzed how algorithms using a single attribute; or as we have called them in this study, QoS-based algorithms, can only be useful to us if RTT, PL or Th are used as part of the criteria for the network selection, one of the benefits of this method is the simplicity in the implementation which will be useful in certain situations but will prove to lack the decision power in other scenarios. We also found that the Decision Function schemes were the most likely to be useful for us because of their flexibility and because they use multi-attribute algorithms to better choose an access network, tools such as WP, SAW or GRA could be used on their own or as part of a bigger algorithm; however, it was also noted that despite being more flexible, being able to use several different attributes may not work in favor for this system due to the limited amount of metrics there are available, such is the case of AHP where it provides a mechanism to rank networks and its attributes but there really is no benefit in using it when there are only a few attributes available. GRA and TOPSIS are complex in their implementation but serve a purpose to rank networks, one by comparing to the best available scenario and the other one by comparing how far each network is from the worst and the best scenarios. Both of these algorithms are quite similar but TOPSIS provides a tool that could be useful at the time of implementing our network decision process as opposed to GRA which due to the limitations in our environment, it is more similar to SAW or WP than to TOPSIS. Continuing down the study Network Intelligence algorithms were described and it was really evident from [40]that these tools benefit greatly from information this system is lacking such as RSS, location, SINR or other different parameters, one of the benefits of using NI is the resolution of complex scenarios but this requires a complex implementation and even more data to feed to the algorithm. NI-based seems to be an interesting solution for deciding handovers in adverse situations or when is critical to save time. Finally context-based schemes have a very obvious requirement to understand the network and its surroundings, by doing this they can predict or manage users and their access points while improving handover times and packet loss; however, this is clearly out of the scope of this project as our terminals are supposed to be isolated from every entity and we can only rely on information it can obtain. All of these systems were studied considering only its applicability, in the next section, the options we've deemed as plausible will be analyzed in conjunction with the Mobile IPv4 protocol and later on with the IPSec tunnels that our system requires.

3.2 Implementation of the Network selection algorithm

This section will cover the process involved in selecting the proper algorithms for further testing. In the first section several considerations will need to be established regarding protocols for the overlay network; MIP and IPSec, and also the metrics that will be measured will be defined in the last segment.

3.2.1 Design considerations

The proposed algorithms will need to consider different aspects that the hardware and overlay networking confine us to. In the first subsection we will explain how MIP and IPSec could

possibly affect the selected algorithms and how to overcome any limitations. Next we will describe the scripting language along with its limitations. In the final subsection, the physical set up for data collection and testing will be described.

3.2.1.1 Applicability with MIP

Several mechanisms have been analyzed which provide the tools to select the best available network; however, most of these mechanisms make use of hardware available counters we could only make use of in one of the interfaces, Figure 3-8A describes this limitation by separating the second MNO from the scope of the information that can be taken from hardware measurements thus we will need to rely on custom made measurements to retrieve information from both interfaces. Another aspect that needs to be taken into account is that Mobile IP is used to provide a mobility to the end user and so it will be running in the background executing its own tasks. Furthermore MIPv4 will be used to source all the user plane traffic and so our network measurement system must run beside this protocol, Figure 3-8B shows this scenario. The work below will deal with the native MIP capabilities of initiating a handover as well as the limitations it includes and, it should provide an overview of the compatibility between the selected network selection schemes and MIPv4.

There are some considerations that the algorithm must work around to, the most evident one is the fact that Mobile IP by itself is already a handover algorithm (section 2.1) that will take into consideration the status of its tunnels in order to steer the traffic. In the current environment there are two RANs and so there will be two mobile IP UDP tunnels from the MN to the HA and because one of these tunnels will have a higher priority than the other one, traffic will always prefer to go through the highest priority tunnel interface. By the proposed standard RFC 5944 the MIP tunnel will remain active for as long as its registration lifetime was set to, this brings a limitation because by Cisco's implementation ([64]) this timer can be set to a minimum of 30 seconds. Cisco; however, has put in place a mechanism to probe the tunnel and bring it down in a more timely fashion and it is done by pinging the HA every

second, after a given amount of failed pings the tunnel will be deemed inactive and traffic will be steered through the second tunnel.

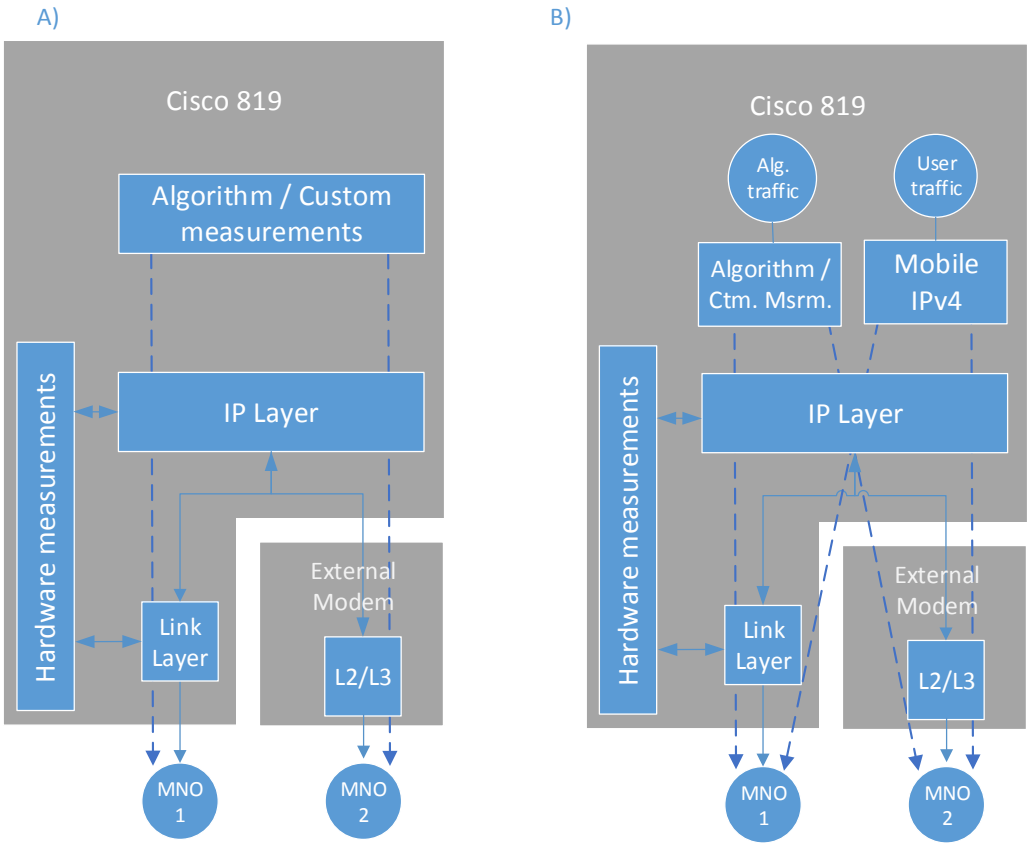

Figure 3-8 - A. Previous architectural assumption for the network selection algorithms. B. New architectural assumption for the network selection algorithms.

It was selected in the previous section that the available attributes for our network selection algorithms are round trip time, packet loss and immediate throughput; however, all these tests need to be run in parallel with the Mobile IPv4 tunnel as seen in Figure 3-9. It will be important to study the impact of this arrangement and the fact that Cisco's MIP implementation already uses packet loss as part of the handover mechanism it uses. The algorithms that will be put to test will be single attribute schemes, the Single Additive Weighting method, the Weighting Products method and the TOPSIS algorithm.

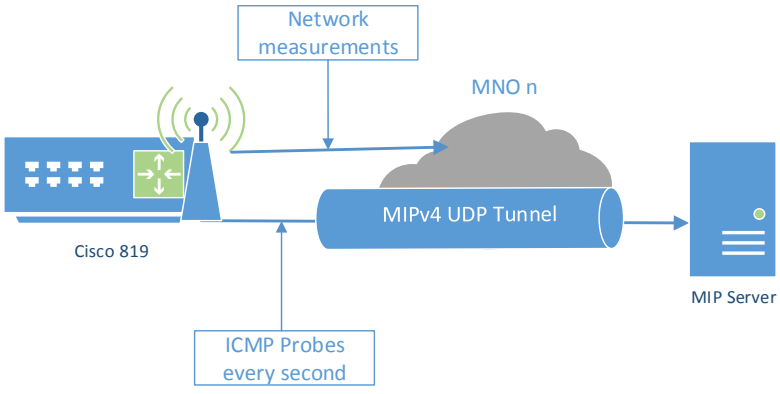

Figure 3-9 – ICMP probes by MIPv4 client in order to keep the UDP tunnel alive.

To method to test the single attribute schemes will be by probing each available network's specific parameter, in this case there will be three tests: RTT, PL and Th. The main objective of this method of selection will be to switchover to the network that provides the highest metric nonetheless it will be needed to know if this type of mechanism will affect or be affected by the Mobile IP handover method, Figure 3-10A showcases this challenge and it is evident how a handover procedure initiated by any of the two selection entities will pose an issue in the work flow of the algorithms. Implementation wise there are no major noticeable concerns but in terms of useful metrics, MIP's tunnel probing is already using PL as network selection parameter; furthermore, because there is a static timeout established for this ICMP probes it can be argued that Round Trip Times of less more than 1000ms will cause the packet to be considered lost, as a result the most useful term to make a network selection would be Immediate throughput, followed by RTT if a low response time is used.

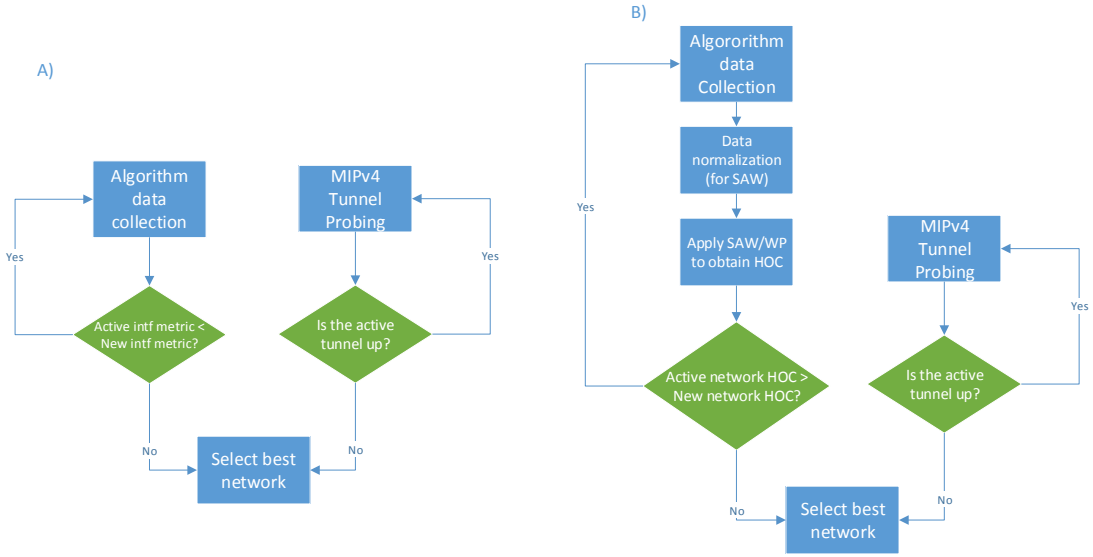

Figure 3-10 - A. Single Attribute scheme algorithm along with MIP handover process. B. SAW/WP mechanisms along with MIP handover process.

The study follows with the SAW and WP methods which will take as produce as outputs what we will call Handover Coefficient (HOC). To take advantage of the benefits provided by these multi-attribute weighting mechanisms RTT, PL and Th ought to be used as data for the network selection. As with the case above, these methods may intervene with the MIP handover and vice versa; as depicted in Figure 3-10B, but this will be a topic for implementation. An important detail with these two options is the fact that the same parameters as MIP's tunnel probing process will be analyzed and so there could be three paths to focus on, one would be using RTT and PL with low weights and so handover initiated by our algorithm won't occur as often just because these metrics are low, the second focus could be one where all attributes have the same weight and so it is equal disruption for the terminal's MIPv4 algorithm and, the last focus could be one where the RTT and PL metrics are weighted high in comparison to Th, this case could try to produce the same results as the MIP process while considering Th in extreme situation, all of this with the ideal of causing less disruption in the system. To finalize this compatibility study with MIP we will use the TOPSIS-based algorithm that was studied in the previous section, as seen in Figure 3-11. When the multi-attribute decision making algorithms were being reviewed, the TOPSIS

framework has a characteristic where it would be preferred to remove the interfaces with very poor performance so they would not affect the ranking of the networks in the actual algorithm, this creates an interesting situation for our environment where both RTT and PL could be used as filters before the actual network selection algorithm makes any network measurements and, if this alternative would be put in place, TOPSIS would be ranking networks based only on immediate throughput.

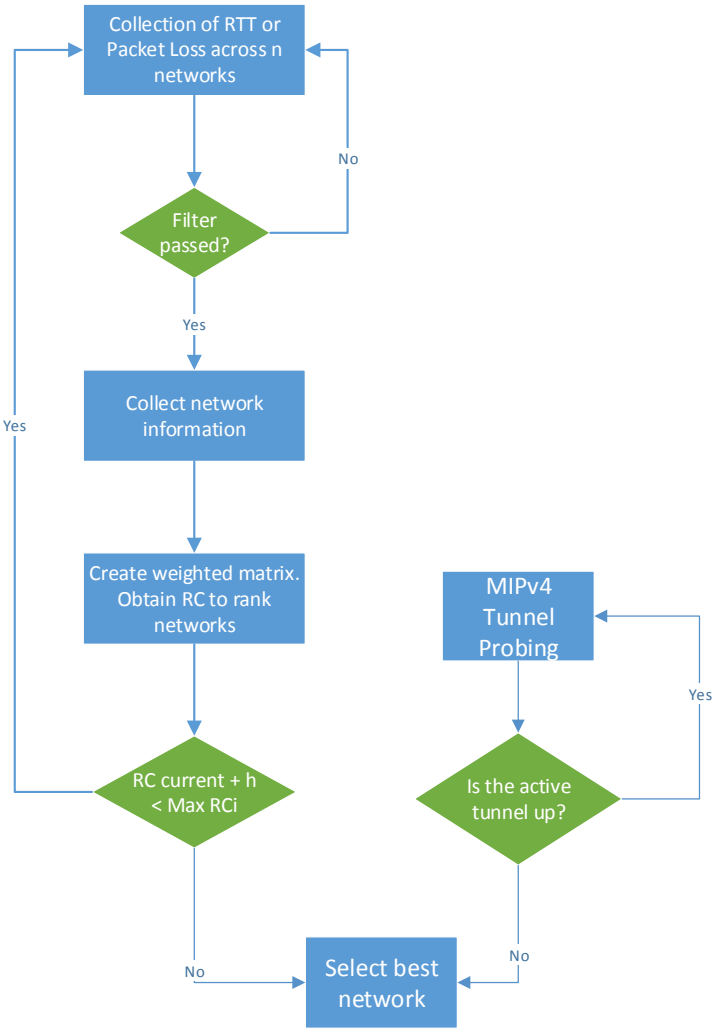

Figure 3-11 – TOPSIS-based handover algorithm.

It is evident that if packet loss and RTT are measured before the actual network selection process comes into place it should keep the system from affecting MIP-related functions and this is more applicable if the frequency in which RTT and PL are measured in our own process is lower than that of MIP's because if the two entities are probing the same poor quality network but one of them is probing faster and can make a decision faster, it should keep the remaining entity from ever triggering; however, it is imperative to notice that this is not a feature of TOPSIS but could also be put to the test in any of the algorithms that will be verified in the implementation stage. At this time a framework has been established where clashes with the MIP Network Selection process need to be minimized or completely avoided and, where it will be better to group RTT and PL on any occasion possible. Next in order is to

complement this MIP analysis with the final stage of this project which is the IPSec tunnel in which all the data will go through, it is important to conclude from this section that IPSec won't affect nor be affected by our algorithm.

3.2.1.2 Applicability with MIP and IPSec

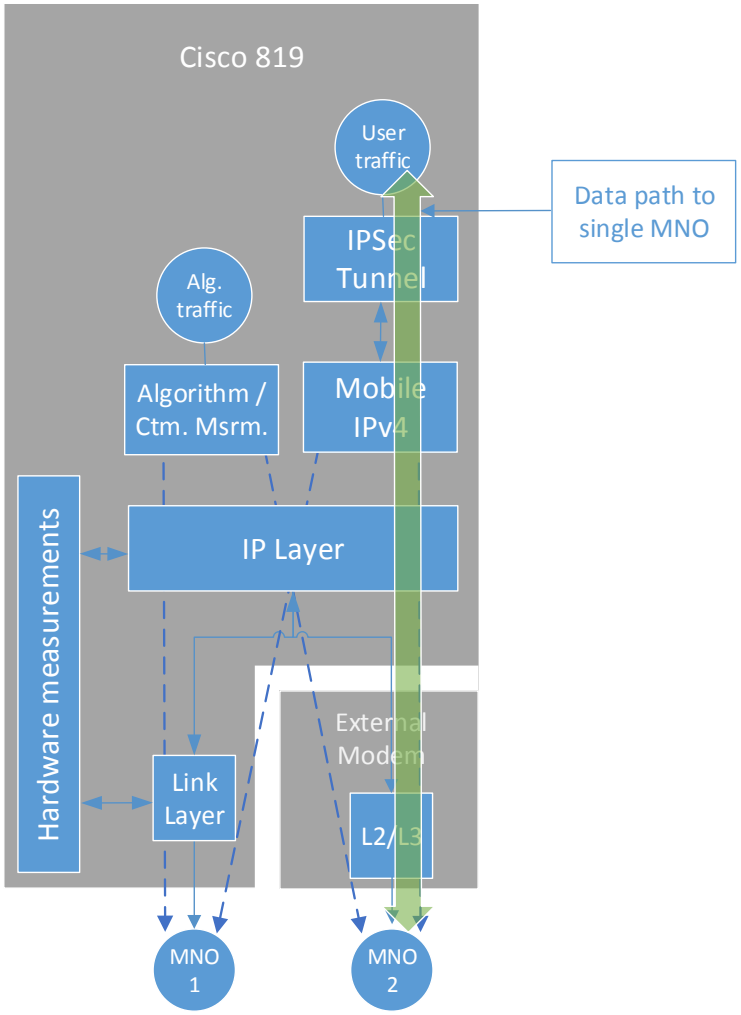

Figure 3-12 - Architectural design of Network Selection Algorithm including MIPv4 and IPSec elements.

It might seem unintuitive to include IPSec in the analysis but because all the data is going through this tunnel there needs to be an important consideration, which was first noted in Figure 2-11A and that is the policy required to send all the traffic into this virtual interface. Any mechanism that will be implemented needs to make sure that the neither the selection algorithm nor the measuring entity fall into the IPSec's traffic policy as otherwise all traffic including our own measuring probes, will go throughout the same MNO as depicted in Figure 3-12. There will need to be a clear separation between these two entities but any limitations that our terminal (Cisco 819) may have will only become apparent during the implementation phase.

In synthesis, regardless of the algorithm implemented there will be a risk to interfere with MIP's network selection function, especially because it is Cisco's implementation of the

protocol and it is not possible to make any adjustments to it. Two mechanisms to minimize conflict were mentioned, the first one (available to SAW and WP) is to consider the RTT and PL with very low or very high weights, that way handover will not occur as often because of these parameters or, it will be triggered in roughly the same frequency as in MIP's tunnel probing. The second mechanism (available to any algorithm that could be implemented) is a filter that will consider these two attributes to select which networks will participate in the network selection process and if the frequency in which these are measured is less than MIP's pattern, this should produce a small amount of times in which the network might be disrupted due to clashing handover triggers, which is the final point in this synopsis. At the time of implementation there needs to be a process that limits the effect of a clashing handover trigger, the issues that this might present are all not so obvious but if there are two handover decisions at the same time; one from the MIP process and the other one from our selection algorithm, the complete handover could take longer than expected due to a ping-pong effect or it could even nullify the choice and switch back to the previous non-optimal interface, Table 3-4 provides a summary of the learnings in this section.

Table 3-4 - MIP and VPN considerations summary.

Implementation framework		
Description	Applies to	Remarks
Using RTT or PL as metrics by themselves will provide no great advantage over the already in place MIPv4 handover process	Single-attribute schemes	If RTT or PL are used, there may be clashes with the MIP handover process
RTT and PL used as filters may be used to ignore very poor performing networks	All schemes	Reduces clashes with MIP handover process thus improving algorithm efficiency
Applying different weights to RTT, PL and Th may reduce clashes with MIP handover	SAW and WP	
Algorithms must isolate themselves from the IPSec traffic policy so as to not probe the same network every time	All schemes	Unknown limitations in the Cisco 819 router

3.2.1.3 TCL Scripting Overview

Based on the considerations obtained from the previous section four mechanisms will be chosen to implement and test their performance. Three of the algorithms will be using the single attribute scheme where RTT, PL and Th will be considered independently, the remaining one will use the proposed RTT plus PL based filter and the network selection done by comparing immediate throughput. The Cisco 819 router is designed to provide basic connectivity functionality to its users and in general, is a very low performing device but with it has the added value to support Tool Command Language, this scripting language allows for interaction with Cisco's own methods and variables in order to reach beyond Cisco's

imposed limitations. TCL is a scripting language that runs within a reserved space in Cisco's operating system IOS and so is restricted from accessing certain internal components.
To run a TCL script, it is needed to access the router's TCL shell which will execute commands on memory (this is no different than Cisco's provisioning language), the scripts can use the available methods to call the router's resources or make use of system events provided by Cisco's Embedded Event Manager (EEM), this tool allows TCL to react based on environmental variables or on information sent or received by the router, Figure 3-13 shows the hierarchy of EEM in IOS.

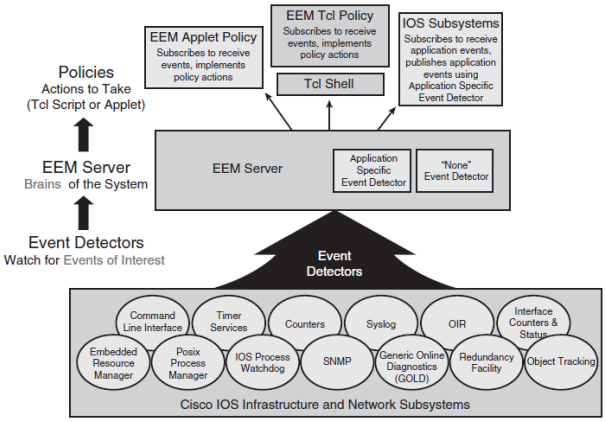

Figure 3-13- Cisco EEM Architecture. Source: [1].

Evidently this poses a challenge in terms of the range of tests available to us as running third party applications is not something allowed by this family of routers; however, what Cisco's TCL does offer is access to its feature set such as interface counters, timers, object tracking and command line interface among others. The algorithms to be implemented will need to be created with this array of tools in such a way that it won't interfere with the router's other functions. There are two alternatives that can be used (Figure 3-14), one is through the use of Cisco Applets which allows for creating a basic TCL script in Cisco's provisioning language, without accessing the aforementioned TCL shell; this method though, provides a limited amount of programming tools and so is not in our interest to use this option, in its place we will run the TCL scripts from the TCL shell; which permits using common scripting language available in TCL 8.4 [65]. In the following section we will review the metrics to be used in the network selection process as well as defining the mechanism how they will be measured, following up with the proposed algorithms.

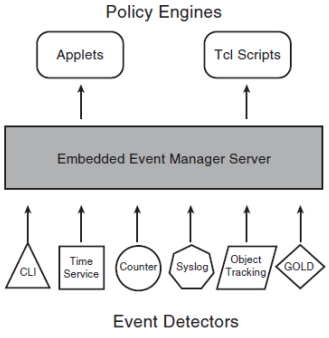

Figure 3-14 - Cisco's TCL implementation options. Source: [1].

3.2.1.4 Physical setup

There will be three sets of equipment to conduct the tests, each set will have a pair of Cisco 819 routers connected in directly via a gigabit interface. The Mobile IP Client will be located in the Cisco 819 3G/WiFi device (Figure 3-15A) while the Cisco 819 4G (Figure 3-15B) device will be used as the external modem. These devices will be connected to the internet via different Public MNOs and through which these will register to the Mobile IP Home Agent and VPN Server, the full specifications for the routers will be located in the Annex section.

Figure 3-15 - A) Cisco 819 3G. B) Cisco 819 4G.

Two of the testing sets is live equipment and data will be collected as part of the normal day to day operations, this will serve to obtain real-life data from a very inconsistent environment; we will call these set of devices MNR01 and MNR02, Figure 3-16 describes how they are set up. The third set of equipment will be sitting static on a desk and will be used to obtain metrics logs as well as running the algorithms; this set up will be called Desk-MNR. Both MNR01 and MNR will be using the same pair of MNOs but they will be geographically distant. Desk-MNR will use different MNOs and will also be geographically distant.

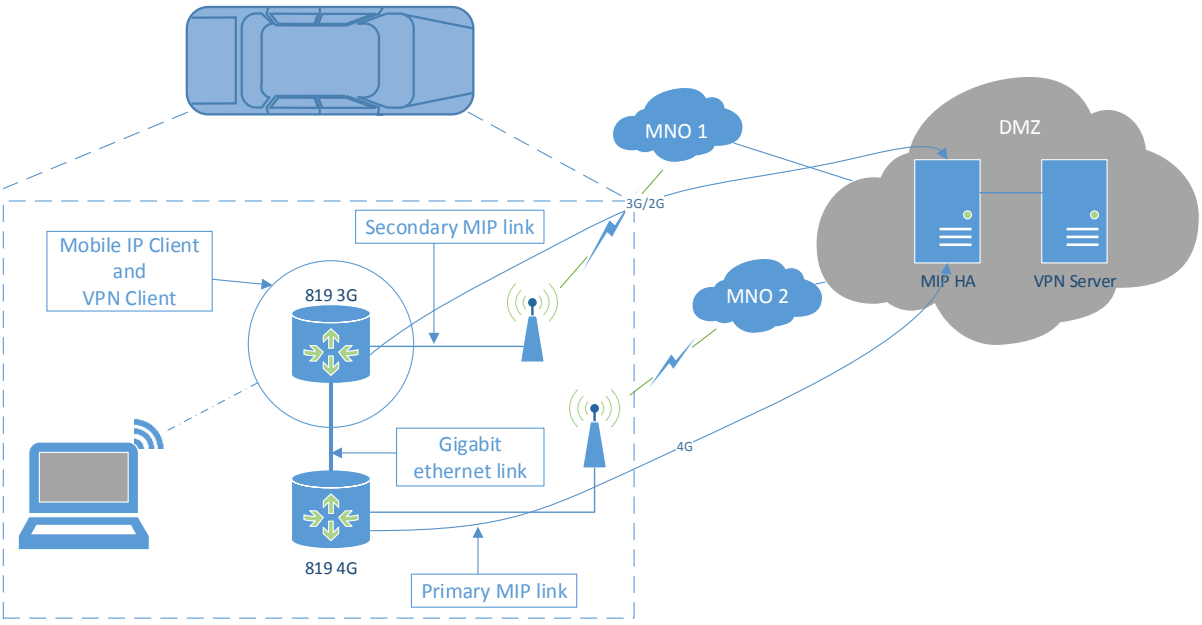

Figure 3-16 - Topology for implementation testing in MNR01 and MNR01. Desk-MNR will have same equipment but it will be on a desk instead of on a vehicle.

For all the tests that will be conducted, the MNR will be using two interfaces connected to different MNOs, these will be called INTF1 and INTF2 as shown in Figure 3-17. In every equipment used for the tests, INTF1 will be the radio interface located in the MIP client device and INTF2 will be the radio interface located in the external router connected via a gigabit cable. In the case of MNR-Desk, there will be an attenuator connected to INTF2 that will be used to force a detrimental state on this MNO's signal strength.

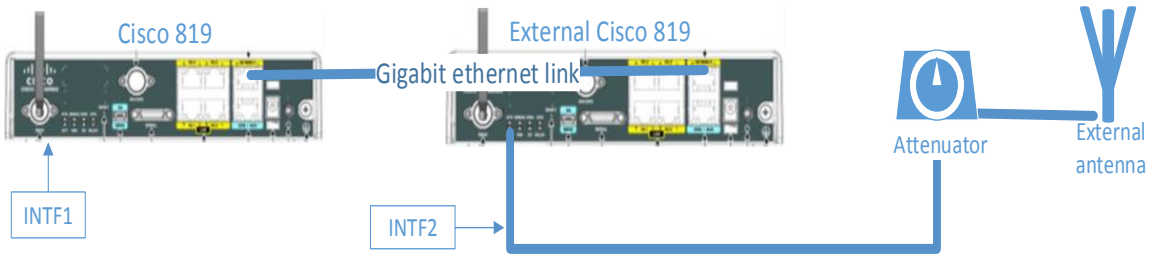

Figure 3-17 - Physical setup of interfaces and antennas.

3.2.2 Defining the Metrics

In this section, we will describe the metrics that will be used as long as the tests that will be carried out to verify their consistency and usability, this will be complimented by the proposed algorithms in the next section and finally the tests will be established.

3.2.2.1 Round-Trip-Time and Packet Loss

Round trip time is the time it takes for a packet to arrive to the defined destination and return to its original owner, in the process there will be several sources of delay affecting the packet, most of these sources are not preventable; such as the time it takes the packet to traverse a given distance or radio interference which would reduce the available bandwidth. Other delay sources will always depend on the network which hosts the terminal and the amount of devices which will need to process the packet before it arrives to its destination and comes back. ICMP has been defined as a tool to verify path to path connectivity and it can be used to measure round trip time very effectively. There are several characteristics that can be given to an ICMP Ping such as the data that it will carry, the length of the payload, Time-to-Live and more, in this case we're more interested in the size of the packet as it will affect buffers throughout the data path. Two different types of pings will be tested, one with a 32B payload and the other one with 1400B. Tests should be made in order to verify the difference in practice between these pings.

Packet loss could be measured based on a response from a server declaring how many packets failed to arrive, protocols such as RTCP (Real Time Control Protocol) contain information on how many packets were sent and how many packets have actually arrived correctly to its recipient. Because one of the ideals of the project is not to include any external network elements this approach shall not be pursued, instead there should be a mechanism that sends a packet and it should expect an acknowledgment per packet. This is effectively a

limitation in our system which we can overcome with the likes of ICMP Ping, by calculating the percentage of ICMP replies.
Measuring both RTT and packet loss percentage with pings would be a waste of resources because of the timeout functionality in ICMP. To elaborate, a ping packet will be declared lost if time equal to the timeout value has passed; this means both that the RTT value is higher than at least 1000 ms and that the packet will be deemed undelivered or lost. We will therefore make use of this relationship and use only RTT in our algorithms.

3.2.2.2 Immediate Throughput

The last metric that will be put to test is the immediate throughput available to the device. This metric could be measured in an active interface by calculating the amount of packets transmitted over an unit of time; however, because it is not possible for the algorithm to control user data and there won't be any information from the inactive interfaces, this approach will not be useful for this case, instead it will be needed to produce load into the system whenever is needed and through both active and inactive interfaces. This approach will use a publicly available server in the internet and download or upload a file using FTP. This tactic will require us to test if the public server enforces some kind of traffic policy such as traffic shaping, time of day preferences or another type of rule that may affect the readings. If the server is in the internet the route a packet will take to it is not readily available and the path might not always be the same; however, if the measurements provide some consistency it should be possible to use this method reliably.

As synthesis, in order to verify RTT and Packet Loss we will make use of the ICMP Echo request and reply functionality readily available in most of the networking equipment. Packet loss testing will be done along with RTT by defining a long round-trip-time value to be taken as a packet loss. The ICMP targets will be determined during implementation along with the address of the public FTP server. The pings will be tested with a one second timeout which matches the MIP value for its tunnel probing and in two different sizes, one with a 32B payload, the other one with 1400B. Packets lost will contribute to the overall increase of the RTT average which will in turn worsen the metric for that interface. Testing immediate throughput will require measuring downlink and uplink speeds, this will be done for three different size of packets: 50KB, 270KB and 1MB which have been chosen arbitrary. In the next section we will describe the physical set up of the implementation tests.

3.2.3 Proposed alternatives

There will be two different metrics to measure, we will implement an algorithm to probe each one of these parameters individually and the third implementation option will be the combined filtering using RTT with inferred packet loss and, the decision will be finally taken based on immediate throughput. It is noted that because the MIP protocol will work without regard of our implementation that there should be a mechanism to obtain which interfaces are

usable every time the algorithm is run, this is what we will be calling the available interface list.

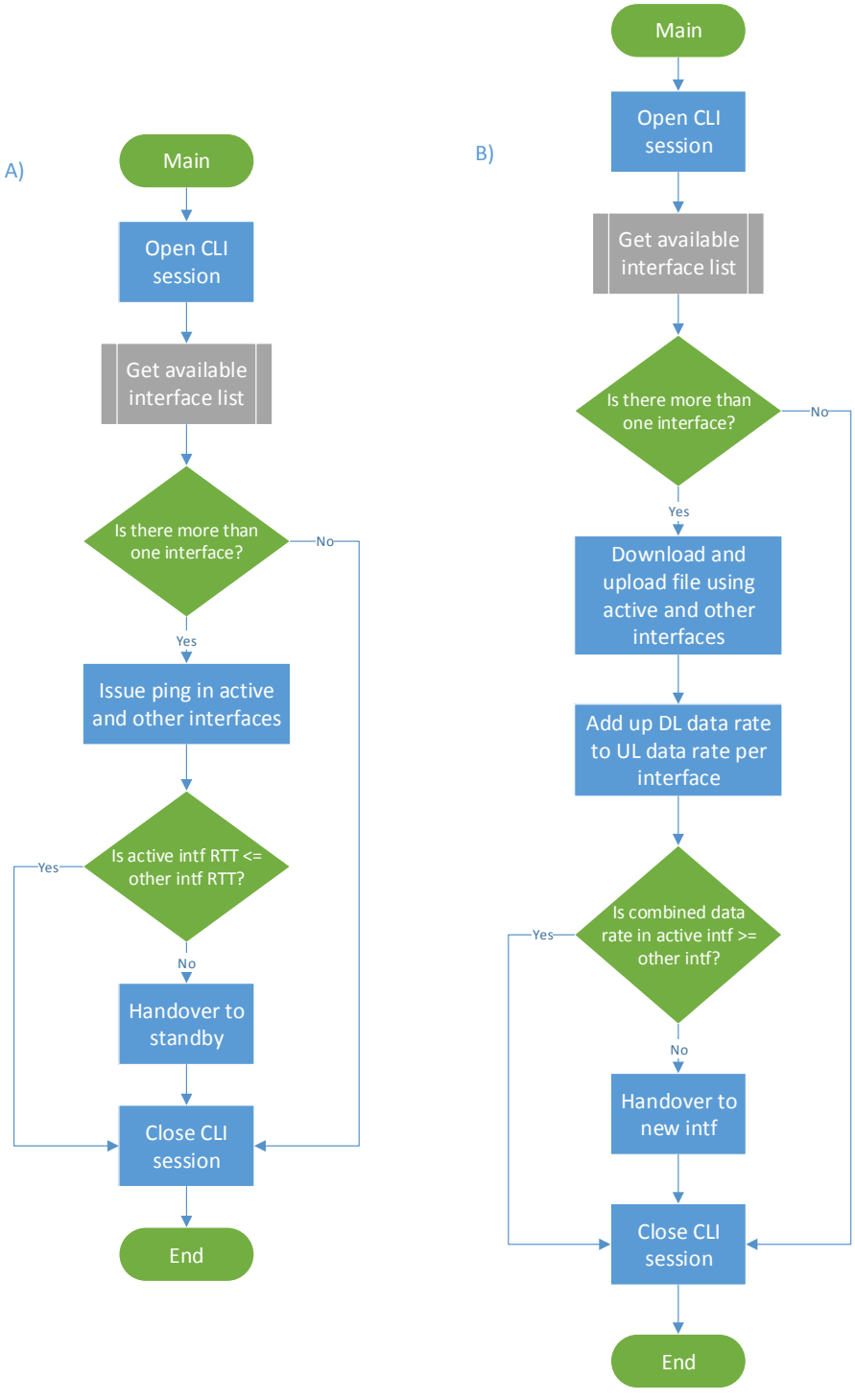

Figure 3-18 - A) RTT-based algorithm. B) Immediate-Throughput-based algorithm.

3.2.3.1 Single Attribute-Based Algorithms

There will be two alternatives described in this section, the first one will make use of Round-trip-time to make a selection on which network to use. The obtained RTT should be an average of more than 1 repetition in order to make the results more reliable. The next single-attribute mechanism will be based on immediate throughput, this means the immediate upload and download data rates will be measured and a network selection will be made based on the obtained results.

RTT-Based Network Selection Algorithm

The objective of this mechanism is to infer how much do buffers increase when the users are located in a poor reception area. If the round trip time to the same destination is roughly the same in a normal functioning scenario, then if access to the network is poor and thus bandwidth is low, packets could suffer higher buffering times, including Ping packets which we will measure and log. In Figure 3-18A we propose the algorithm to be implemented and in Figure 3-19 we can see the pseudo code. The mechanism can be customized by changing the amount of repetitions and capturing the average RTT value, changing the size or changing the timeout to deem a ping undelivered. It was stated in the previous chapter that initial section that it is recommended to keep this timeout lower than or equal to one second as this is the value that Mobile IP uses to probe its tunnel. The algorithm will compare the RTT of the interface with the lowest value to the RTT of the active interface and change interfaces if the active one performs worse.

```
1  initialize cli_session
2  interface_list = get_available_interface_list
3  active_intf = get_active_intf from interface_list
4  IF  interface_list is NOT empty THEN
5      initialize ping with n repetitions, m size and o timeout
6      WHILE interface_list NOT empty
7          route traffic through first interface in interface_list
8          round-trip-time = get_rtt_from( ping $interface )
9          IF round-trip-time is empty OR higher than 1000ms THEN
10             SET round-trip-time to 999 ms
11         ELSE
12         END IF
13         add to rtt_array [ interface_name, round-trip-time ]
14         POP row from interface_list
15     ENDWHILE
16 ELSE
17     EXIT
18 END IF
19 POP active interface row from rtt_array
20 SORT rtt_array based on highest
21 IF active_interface_rtt lower than or equal to first entry in rtt_array THEN
22     EXIT
23 ELSE
24     initiate handover to interface_name in first entry in rtt_arry
25 END IF
26 close cli_session
```

Figure 3-19 - Pseudo code for RTT-based algorithm.

Immediate Throughput-Based Algorithm

In this third single attribute algorithm a file will be downloaded and uploaded to a public internet server in order to obtain the total throughput available at that given moment in time. This public server should be consistent enough in the sense that data rate speeds should not vary greatly under normal operations. As is noted in the process flow (Figure 3-18B) and in the pseudo code (Figure 3-20), the upload and download process will take place separately and independently due to limitations in Cisco software. The sum of uplink and downlink data rates will be the value to be used as comparison and consequently the network selection.

```
initialize cli_session
interface_list = get_available_interface_list
active_intf = get_active_intf from interface_list
IF  interface_list is NOT empty THEN
    initialize file with file_name
    initialize server with server_address
    WHILE interface_list NOT empty
        route traffic through first interface in interface_list
        dl_datarate = get $file download speed from $server
        ul_datarate = get $file upload speed to $server
        throughput = download speed plus upload speed
        add to th_array [ interface_name, throughput ]
        POP row from interface_list
    ENDWHILE
ELSE
    EXIT
END IF
POP active interface row from rtt_array
SORT rtt_array based on highest
IF active_interface_th higher or equal to first entry in th_array THEN
    EXIT
ELSE
    initiate handover to interface_name of first entry in th_array
END IF
close cli_session
```

Figure 3-20 - Pseudo code of immediate-throughput-based algorithm.

3.2.3.2 Multiple Attribute Network Selection Algorithm

The final alternative that will be proposed makes use of the three aforementioned metrics in an attempt to initiate the network selection process less often. The algorithm is divided in two main sections, the network selection process and the interface filtering process. In Figure 3-22, filtering will occur when the interface list is updated, if there are no usable interfaces in this new list then the network selection process will not proceed and the algorithm will end there. This filter is supposed to mimic the RSS based network selection filter step from many of the studied algorithms in the previous section. What concerns us in this case is the actual filter, which is done by issuing Pings and comparing the RTT and packet loss percentage, if it doesn't exceed a pre-established threshold then this interface won't participate in the

handover, this information can be observed with more detail in the pseudo code in Figure 3-21.

```
initialize cli_session
interface_list = get_available_interface_list
active_intf = get_active_interface from interface_list
WHILE interface_list NOT empty
    initialize ping with n repetitions and m size
    route traffic through first interface in interface_list
    round_trip_time = get_rtt_from( ping $interface )
    IF round-trip-time is empty OR higher than 1000ms THEN
        SET round-trip-time to 999 ms
    ELSE
    END IF
    IF round_trip_time LESS THAN n THEN
        add to updated_interface_list
        pop row from interface_list
    ELSE
        pop row from interface_list
    END IF
ENDWHILE
IF  updated_interface_list is NOT empty THEN
    initialize file with file_name
    initialize server with server_address
    WHILE updated_interface_list NOT empty
        route traffic through first interface in updated_interface_list
        dl_datarate = get $file download speed from $server
        ul_datarate = get $file upload speed to $server
        throughput = download speed + upload speed
        add to th_array [ interface_name, throughput ]
        POP row from interface_list
    ENDWHILE
ELSE
    EXIT
END IF
POP active interface row from th_array
SORT th_array based on highest
IF active_interface_th higher or equal to first entry in th_array THEN
    EXIT
ELSE
    initiate handover to interface_name of first entry in th_array
END IF
close cli_session
```

Figure 3-21 - Pseudo code for the multi-attribute network selection algorithm.

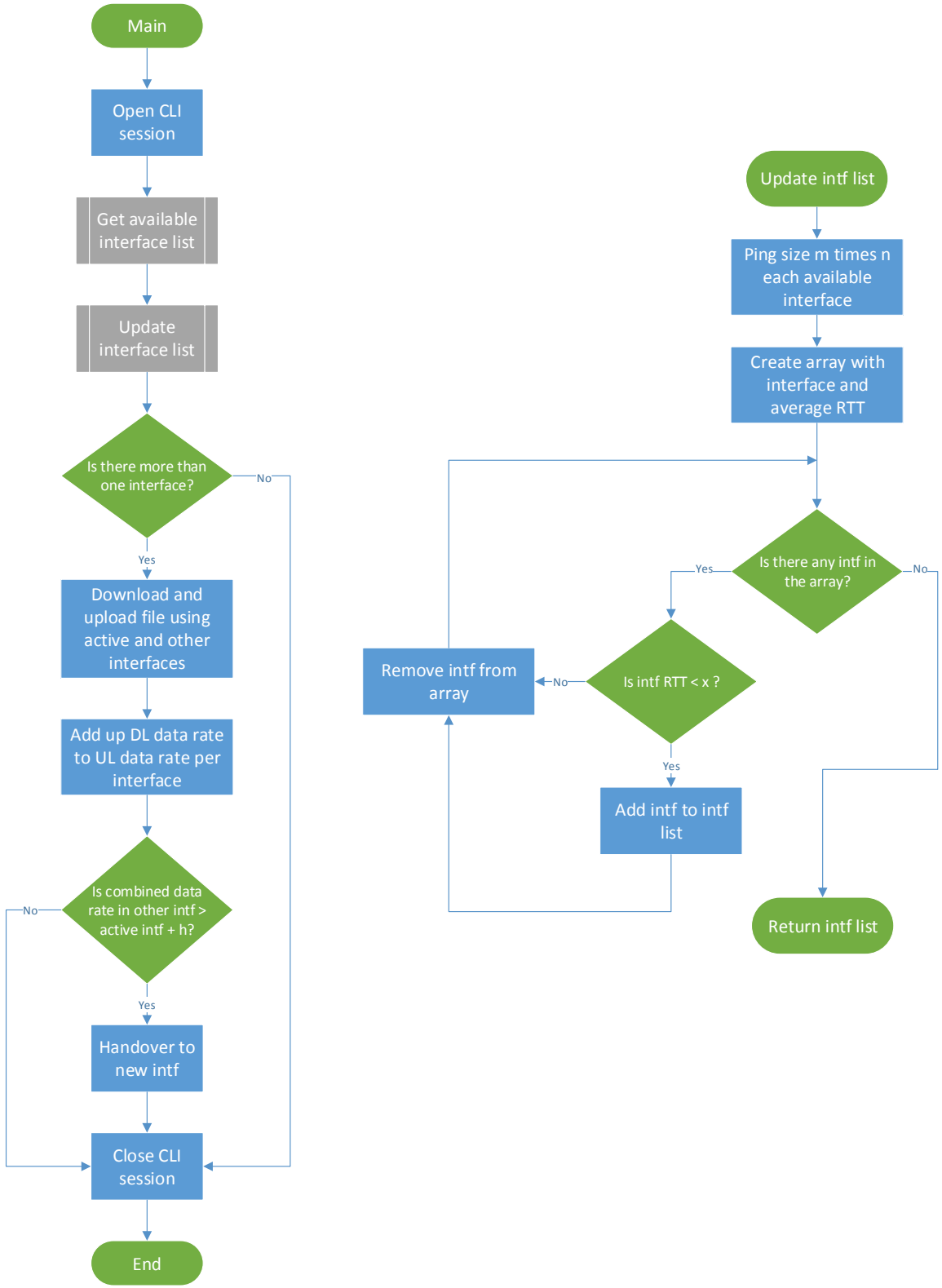

Figure 3-22 - Multi-attribute network selection algorithm.

3.2.4 Testing

At this point, we have defined the attributes and the algorithms to implement and compare; however, as it was stated in the previous sub-section we will need to select the characteristics

of the measurement device. In this first section we will compare two different sizes of pings to the same target, one with 32B and the other one with 1400B as payload. These pings will then be compared against data rate to verify if there is any correlation. Finally a selection of what ping or type of pings will be made. In the second sub-section we will measure the difference in download and upload speeds and study which one; if any, would provide the most accurate result.

3.2.4.1 Defining the Characteristics of the RTT-Measurement-Device

RTT Tests on MNR-Desk

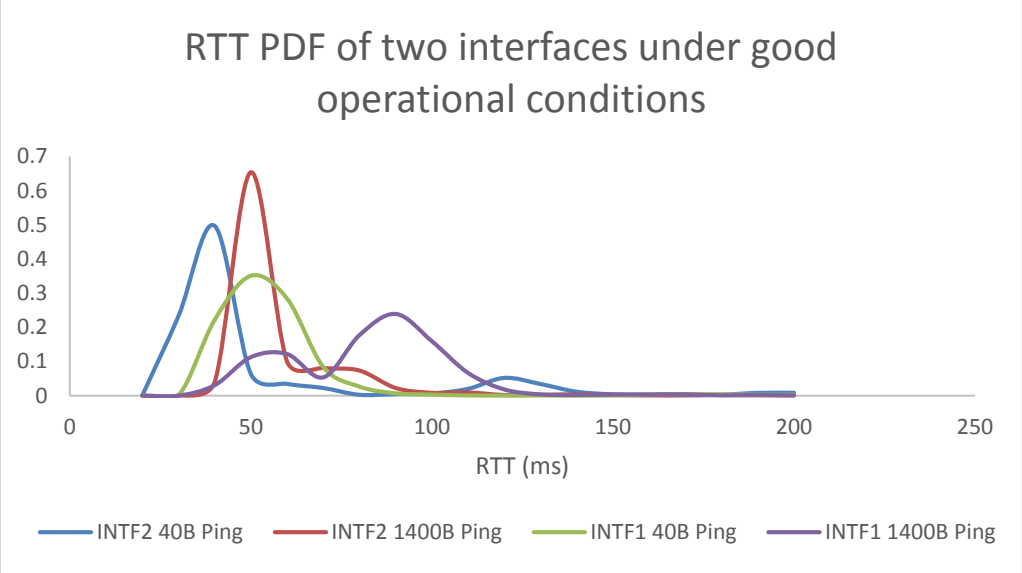

Figure 3-23 - CDF of RTT values on normal operational conditions.

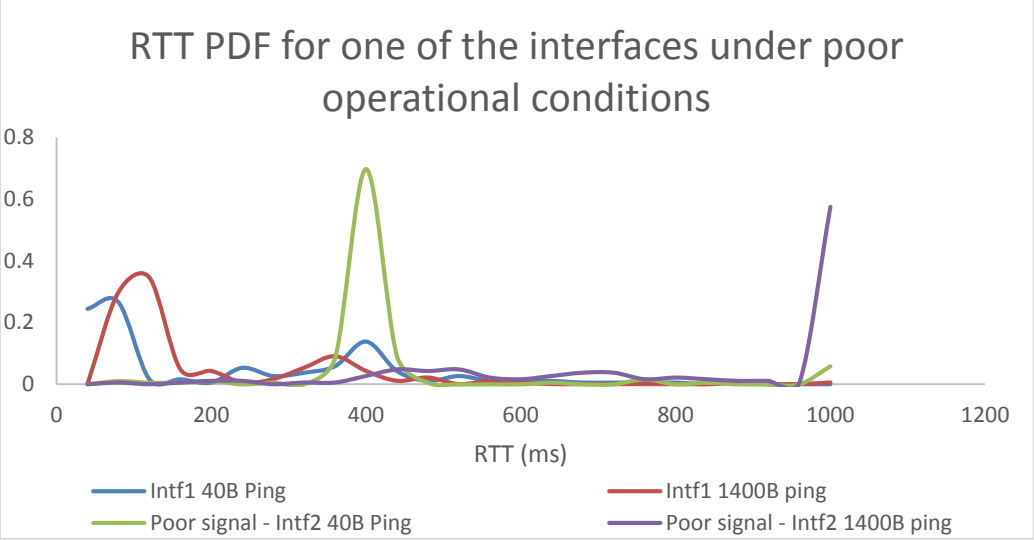

Figure 3-24 - CDF of RTT values with one interface subject to attenuation.

These tests will service to verify the difference in RTT values for our test device when using the attenuator to worsen the signal strength on INTF2. Figure 3-23 shows how it looks when there is no external force working on the modems, Figure 3-24; however, shows that the probability distribution for INTF2 when there is poor signal is heavily skewered to the right of the graph where RTT values are higher. This means we can rely on the attenuator forcing a detrimental state on INTF2.

MNR2 User Plane Data Effect on ICMP Messages

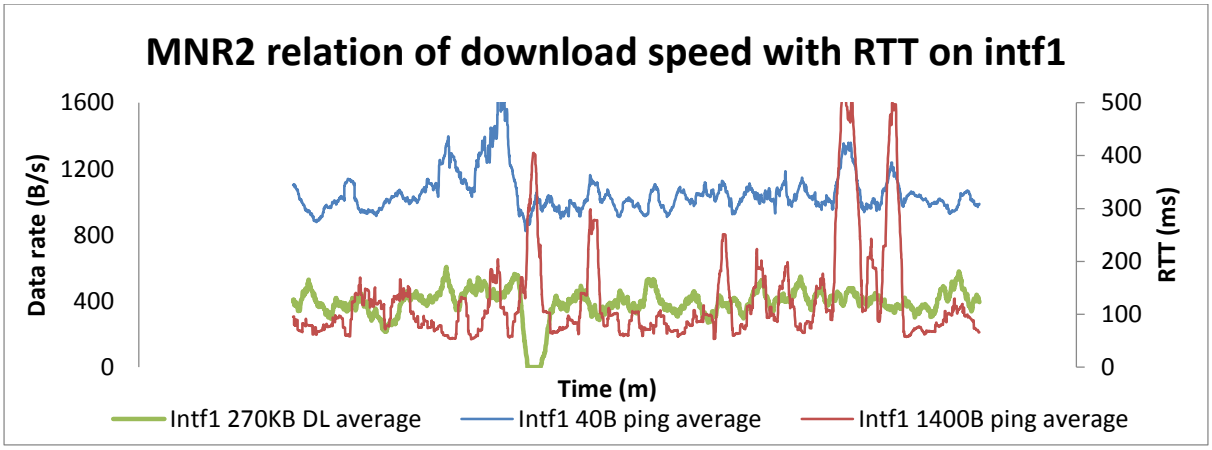

Figure 3-25 - Relationship of RTT values with DL rate on INTF1

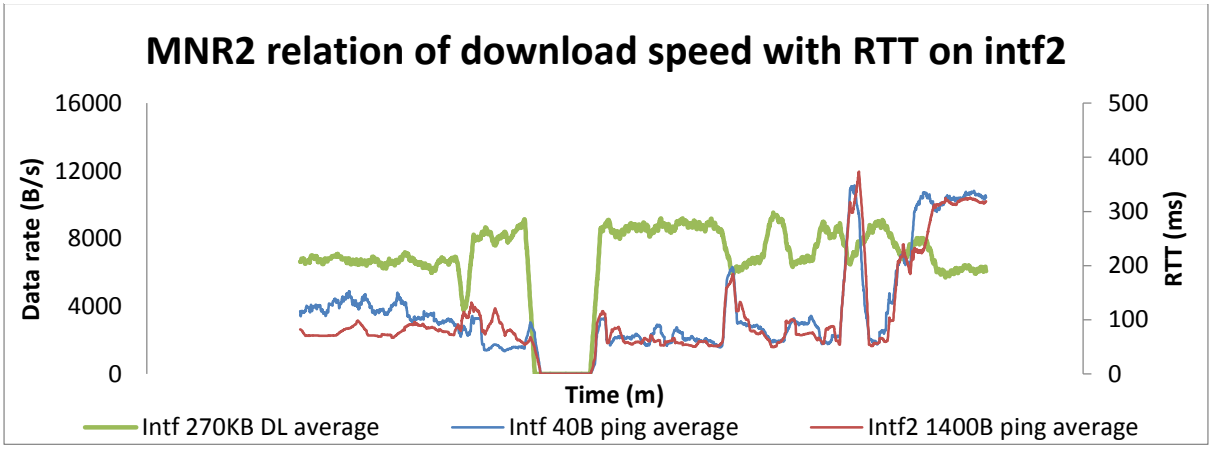

Figure 3-26 - Relationship of RTT values with DL rate on INTF2.

The images above show the effect that a download has over the ICMP-based round-trip-times. In the first case, it's noted that there is a positive correlation where whenever, data rate increases, RTT decreases, this is likely because the signal strength for this router. This is true for both interfaces, as there is really no effect from actual user traffic on the ICMP messages' RTT.

3.2.4.2 Defining the Characteristics of the Immediate Throughput Measurement Device

In this sub-section, different tests will be made to determine the most reliable test to perform on the mobile routers. Different file sizes will be downloaded and uploaded to and from the same network devices and in the end we should be able to see what tests will be useful to implement.

File Upload and Download Tests in MNR1 and MNR-Desk

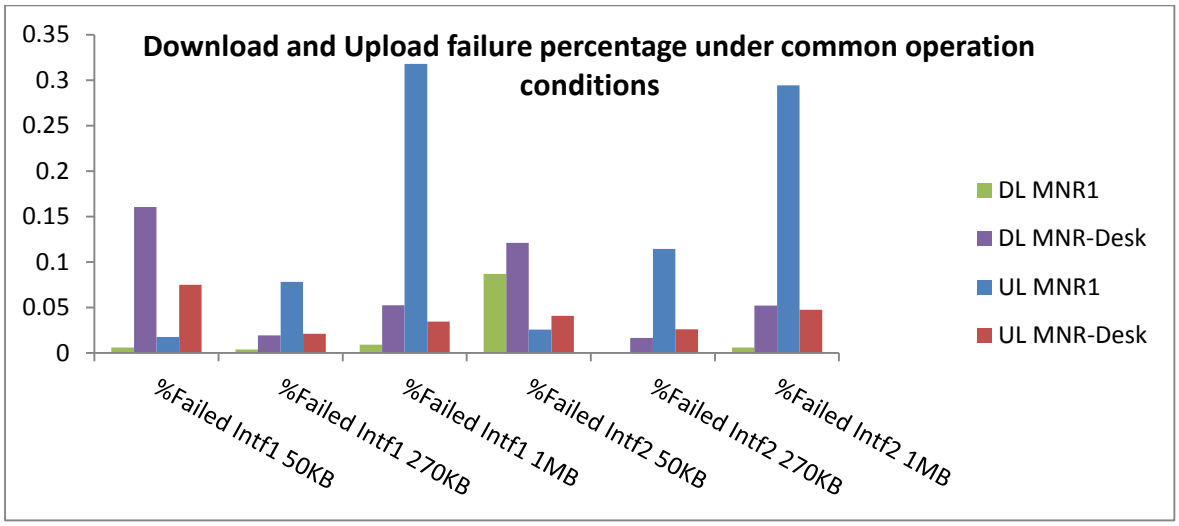

Figure 3-27 - Percentage of failed upload and download tests.

During the tests, it was clear that the percentage of failed upload from the testing routers was too big to continue to be used as part of the tests. In general, the upload procedure was dropped out and it was decided that download speeds will be used for the proceeding tests with the algorithms.

Download Speed on MNR-Desk with Low Signal Strength in INTF2

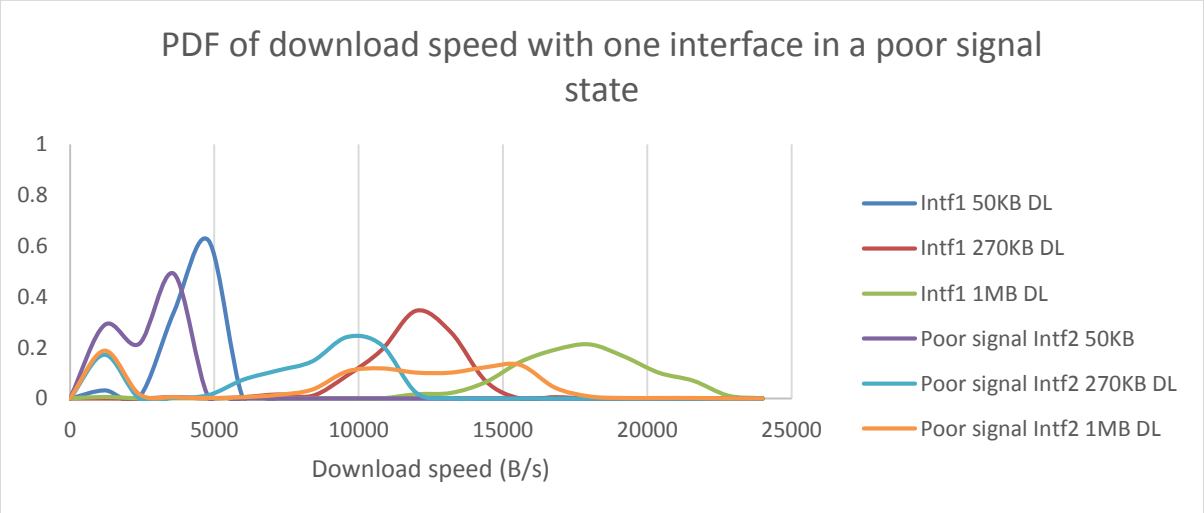

Figure 3-28 - PDF of DL rate when one interface is subject to attenuation.

The test above the difference in download speeds between INTF1 and disrupted INTF2 (Figure 3-28). The focus on this test is to verify which of the file size provides the most room to differentiate between the two interfaces. As an example, a 50KB file downloaded on INTF1 with a rate of 5 KB/s 63% of the times, but on INTF2 49% of the times, the file was downloaded at 3.6 KB/s. We consider this difference to be too small to make any network selection decisions and so we've chosen to use 270KB files to proceed with our tests.

Download Rate of 270KB File across Testing Devices and Interfaces

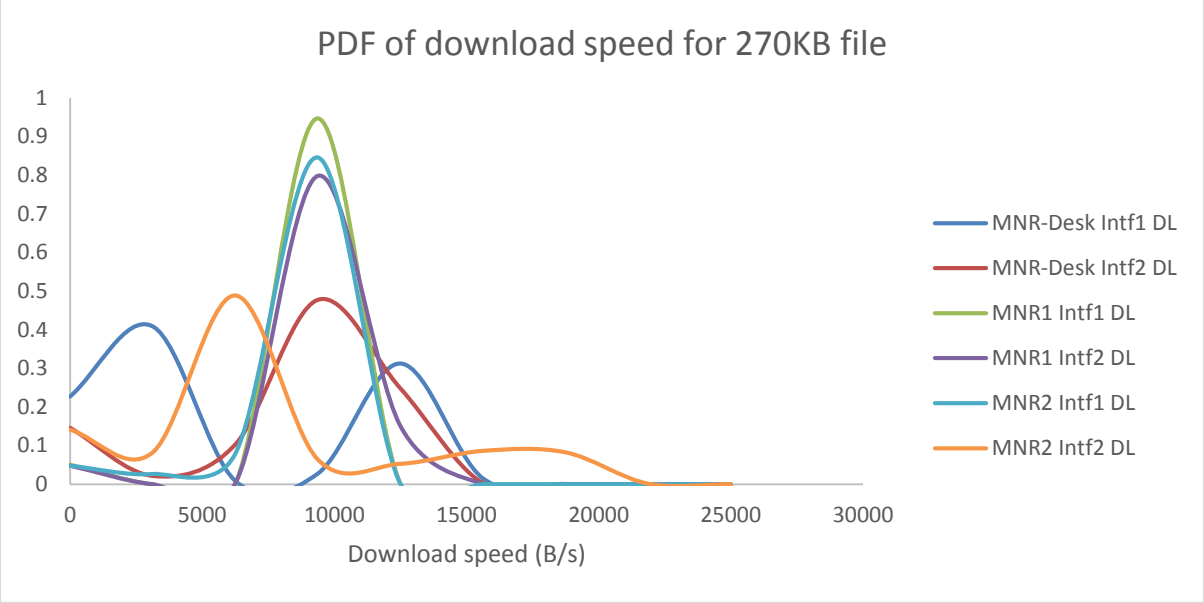

Figure 3-29 - Distribution of DL rates of a 270KB file on different devices and interfaces.

Figure 3-29 shows the percentage of download values for the 270KB file when all interfaces are under normal operational conditions and there is no attenuation done on MNR-Desk. Clearly MNR2-INTF2 and MNR-Desk-INTF1 have the lowest download rates and most of the values are less than 10 KB/s. Interestingly MNR2 is usually subject to a lower performance on INTF2 and this shows in this test.

3.2.5 Scenarios to Verify

We have established that RTT can be differentiated well enough if the signal strength is degraded in one of the interfaces. We have also established that the immediate throughput tests will be done using by downloading a 270KB file across the two available interfaces in the MNRs.

All the tests will be done on MNR-Desk and the scenarios that need to be verified are the following:

1. What is percentage of false positives when using Mobile IP and INTF2 is subject to attenuation?
2. What is the data rate for a 40B ping RTT-based network selection algorithm when INTF2 is subject to attenuation?
3. What is the data rate for a 1400B ping RTT-based network selection algorithm when INTF2 is subject to attenuation?
4. What is the data rate for an immediate throughput-based network selection algorithm when INTF2 is subject to attenuation?
5. What is the data rate for a multi-attribute algorithm when INTF2 is subject to attenuation?

4 Results

In this section, the results from implementing the network selection algorithms will be displayed and analyzed. In the first section there will be a comparison of all the mechanisms used along with their optimization parameters. Afterwards, there will be a ranking of the algorithms that should provide an answer as to what type of algorithm is useful for our current goals.

4.1 Comparison

The tests that follow in the next sub-sections were performed by applying the network selection algorithm to the set of data collected over three weeks. This allows us to compare the algorithms and rank them in the following section.

4.1.1 Percentage of False Positives when Using Mobile IP and INTF2 is Subject to Attenuation

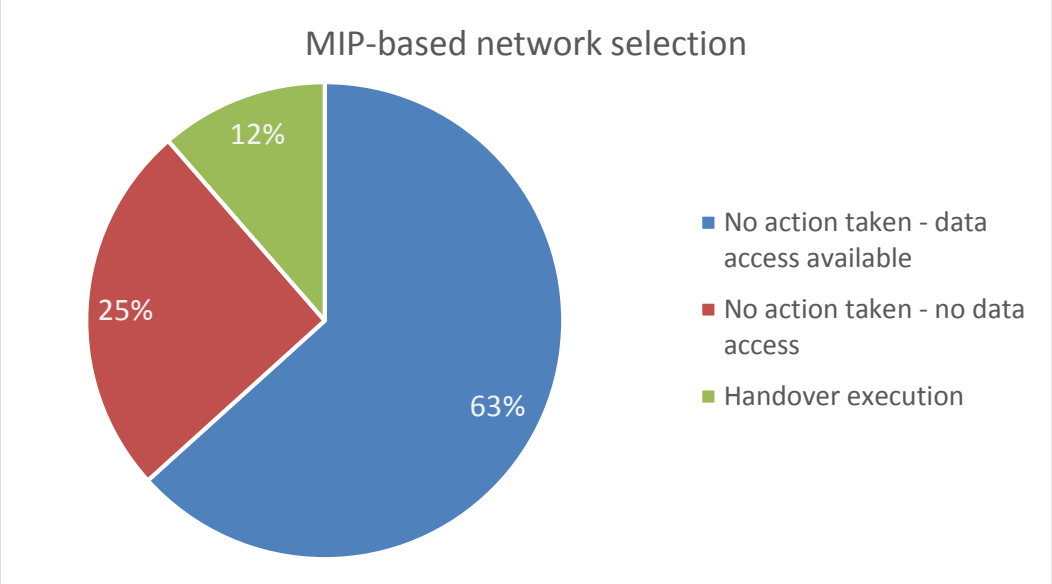

Figure 4-1 - MIP network selection.

When there are no network selection algorithms in place and one of the interfaces is experiencing heavy degradation of its signal, Mobile IP may sometimes not perform a handover to a network that has data access, this is due to the fact that MIP only has its ICMP keepalives to make its choice. Figure 4-1 shows that there is 25% chance of using a network with no data access available to the end user. The focus of the tests to follow will be to make a better network selection when data rate available to the end user is poor by making use of different measurements and comparing the results from all the available interfaces.

4.1.2 Data Fate for a 40B Ping RTT-Based Network Selection Algorithm when INTF2 is Subject to Attenuation

The results from the average RTT values for 40B pings can be found in Figure 4-2. These values are fed into the algorithm and a network selection will be made according to the interface that has the best Round trip time. In Figure 4-3 it's possible to see that the algorithm can be optimized for different values of RTT, the optimization that provided the highest data rate when the base case was the lowest is found for values under 300ms. This means that when the interface RTT is less than 300 ms, there is a higher probability to make use of a better network. Using 300ms as threshold also means that network selection is more volatile because it allows for a smaller window of variation in the RTT measurements. Making use of any other optimization results in better connectivity some of the times but grants more flexibility in the event of unexpected RTT values.

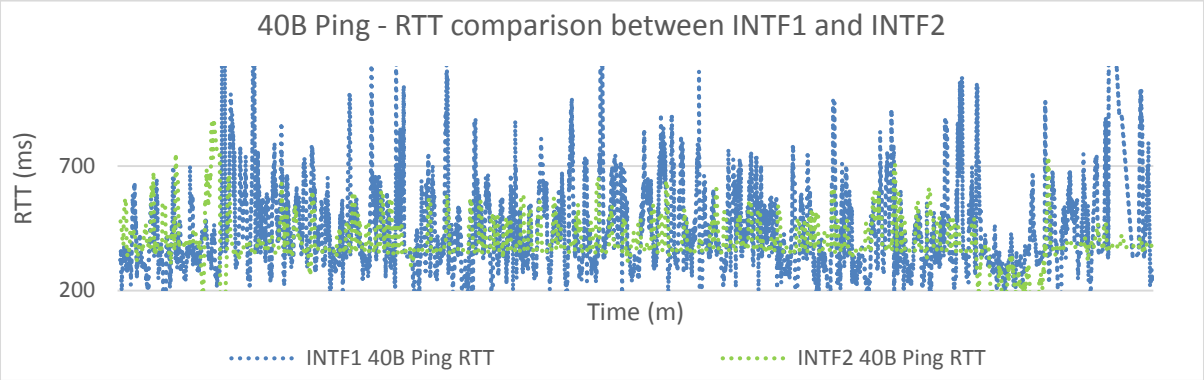

Figure 4-2 - Measured RTT values for 40B pings.

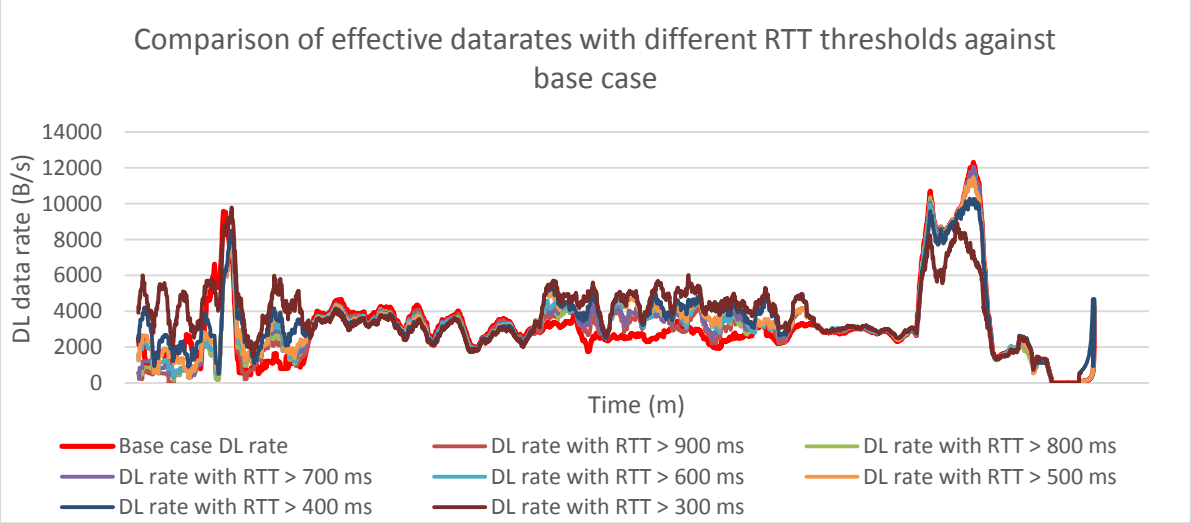

Figure 4-3 - Obtained data rate using the RTT-based algorithm using 40B pings.

4.1.3 Data rate for a 1400B Ping RTT-Based Network Selection Algorithm when INTF2 is Subject to Attenuation

As with the previous section, this test makes use of the RTT-based algorithm but this time utilizing 1400B pings instead of 40B ones. Figure 4-4 shows the RTT measurements taken using a 1400B ping and Figure 4-5 displays the data rate obtained for the different optimizations of RTT values. It is noticeable that most of optimizations done with this test result in data rates worse of those from the base case. RTT values of less than 300ms once again result in good data rate for part of the measurements but can also induce a poor experience for the end user due to its small window for RTT to vary.

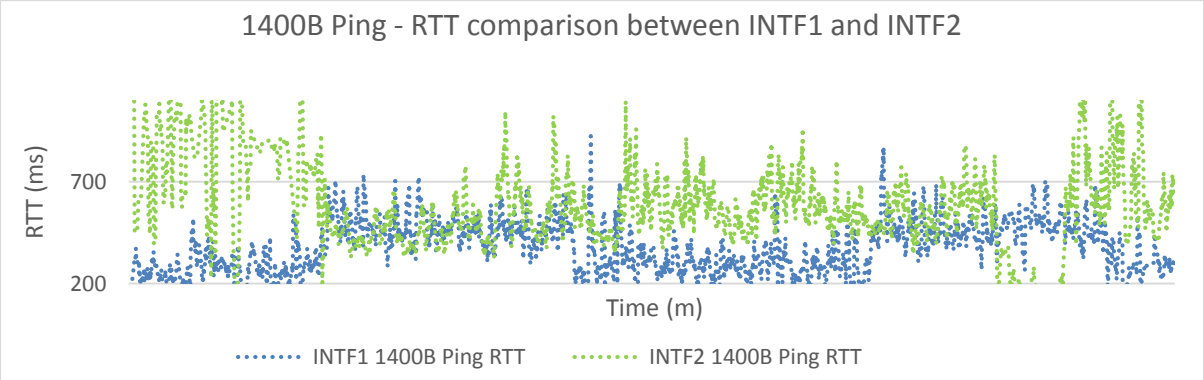

Figure 4-4 - Measured RTT values for 1400B pings.

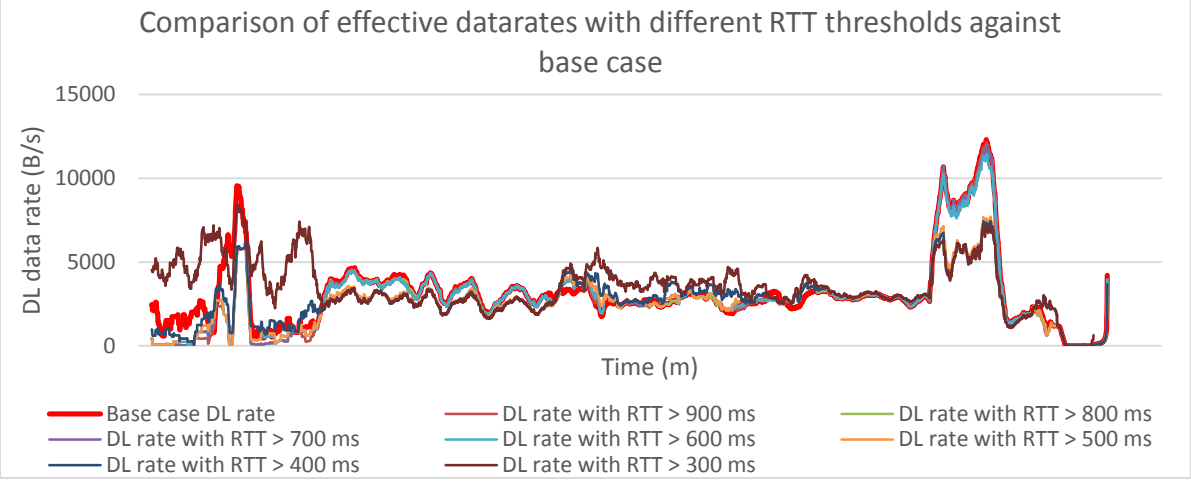

Figure 4-5 - Obtained data rate using the RTT-based algorithm using 1400B pings.

4.1.4 Data Rate for an Immediate Throughput-Based Network Selection Algorithm when INTF2 is subject to Attenuation

These tests were made making use of the immediate throughput-based algorithm, in the section 3.2.4 was decided that a download of a 270KB file will be reliable enough to be used for our tests. Figure 4-6 shows what the measured data rate when downloading such file is, this is information will then be fed into the network selection algorithm to decide which interface to use. The available data rate using this algorithm can be optimized based on the obtained measured download speed, Figure 4-7 displays the different data rates resulting from varying the immediate throughput threshold. Because the available data rate is measured through the download of these files, this algorithm naturally selects the network providing the most throughput in most cases. One case that stands out is when throughput is less than 1.25KB/s the best network is chosen at all times, this is in contrast to using a high threshold such as 8.75KB/s where there are fewer opportunities that this data rate will be reached and also, if no data rate reaches the threshold there is the default choice to move to INTF2.

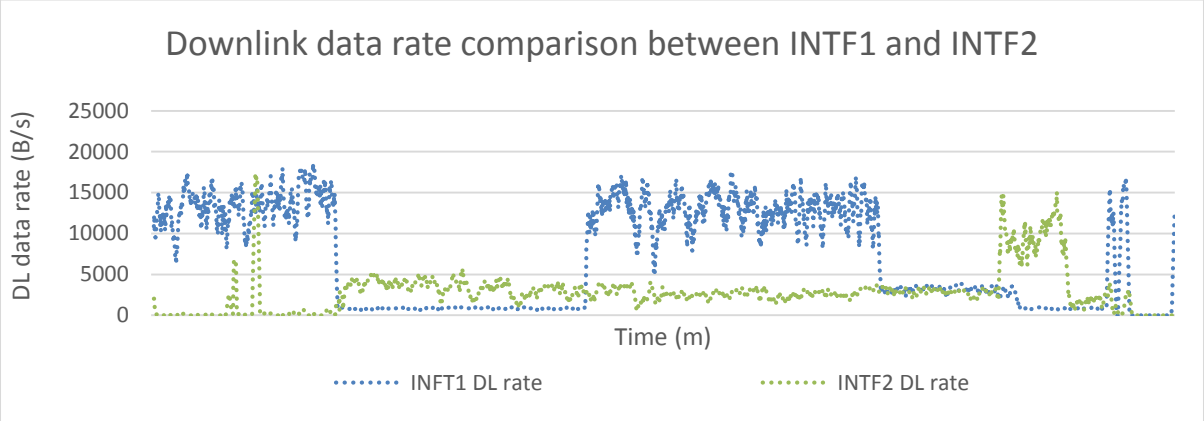

Figure 4-6 - Measured data rate in INTF1 and INTF2.

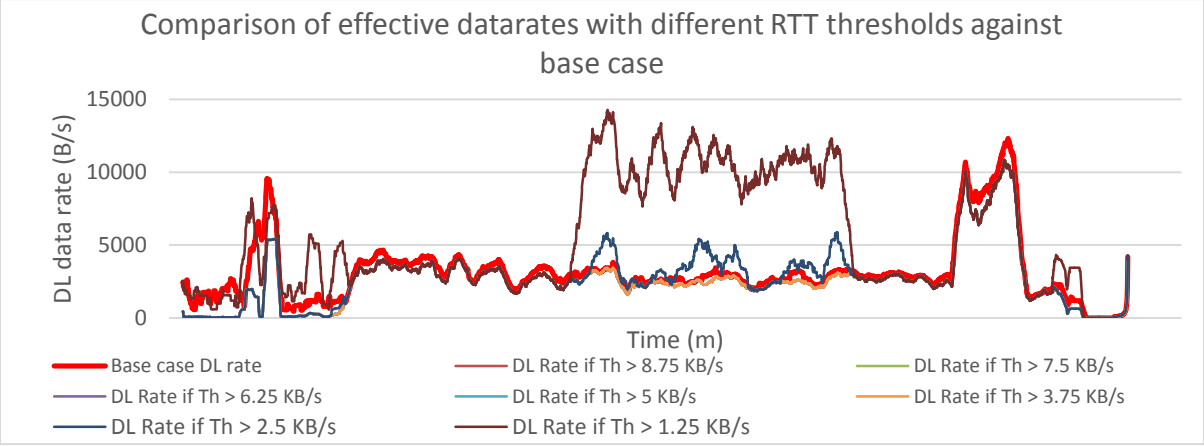

Figure 4-7 - Obtained data rate using the throughput-based algorithm.

4.1.5 Data Rate for a Multi-Attribute Algorithm when INTF2 is Subject to Attenuation

The multi-attribute algorithm makes use of both RTT and immediate throughput measurements to make its network selection. The resulting behavior can be found in Figure 4-8 where a more diverse set of optimization options are available. From this date is possible to see that making use of a 1400B results in the highest obtained data rate for most of the test and this is true for most of the RTT values, except when RTT is less than 900 because this particular value encompasses most of the measured round trip times. Making use of the multi-attribute algorithm doesn't achieve the best results as seen when making use of throughput alone; however, it allows for greater flexibility, less transferred data and decreased handover time, as it will be seen in the section 4.2 when the results will be analyzed and there will be a ranking of the tested networking algorithms.

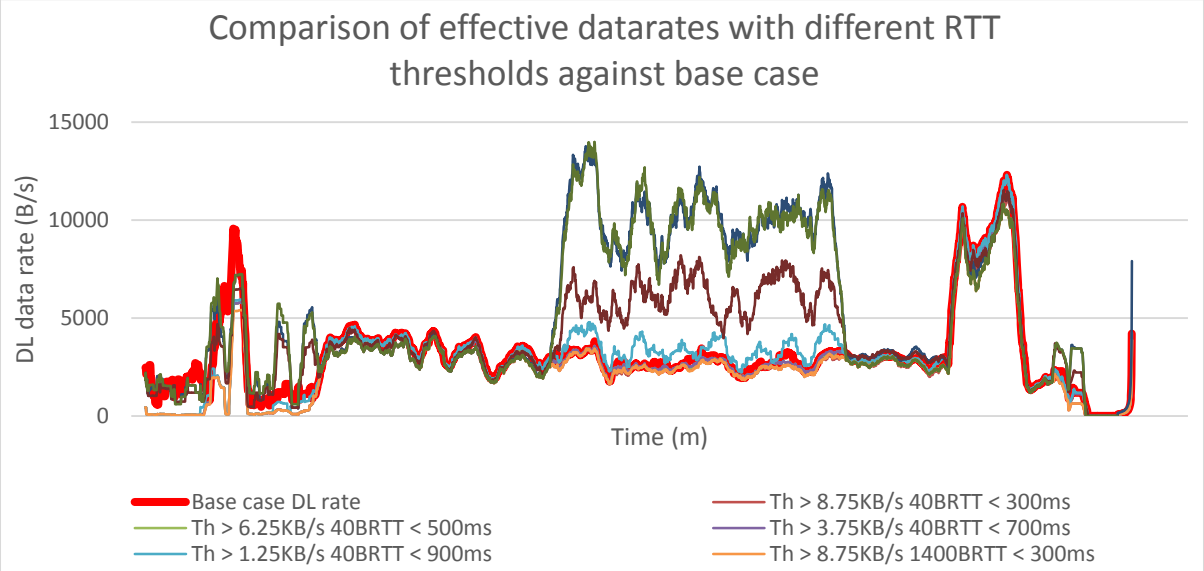

Figure 4-8 - Data rate obtained using the multi-attribute algorithm.

4.2 Ranking of Network Selection Algorithms

Now that the data rates for all the network selection algorithms have been analyzed, next in order there will be a ranking of the mechanisms in order to judge them not only for its results but for the costs (money or time wise) they imply.

In Figure 4-9 we can find the cumulative distribution function (CDF) and the probability density function (PDF) of the obtained data rates from all the different tests done in section 4.1. Looking at the CDF is possible to see that the majority of the results are close to the 3.75KB/s area; however, the best algorithms grant more results continuing right in the X-axis,

for RTT-based schemes, this benefit is minimum whereas for the throughput-based algorithm or the multi-attribute algorithm, there is a noticeable increase in the 20KB/s area.

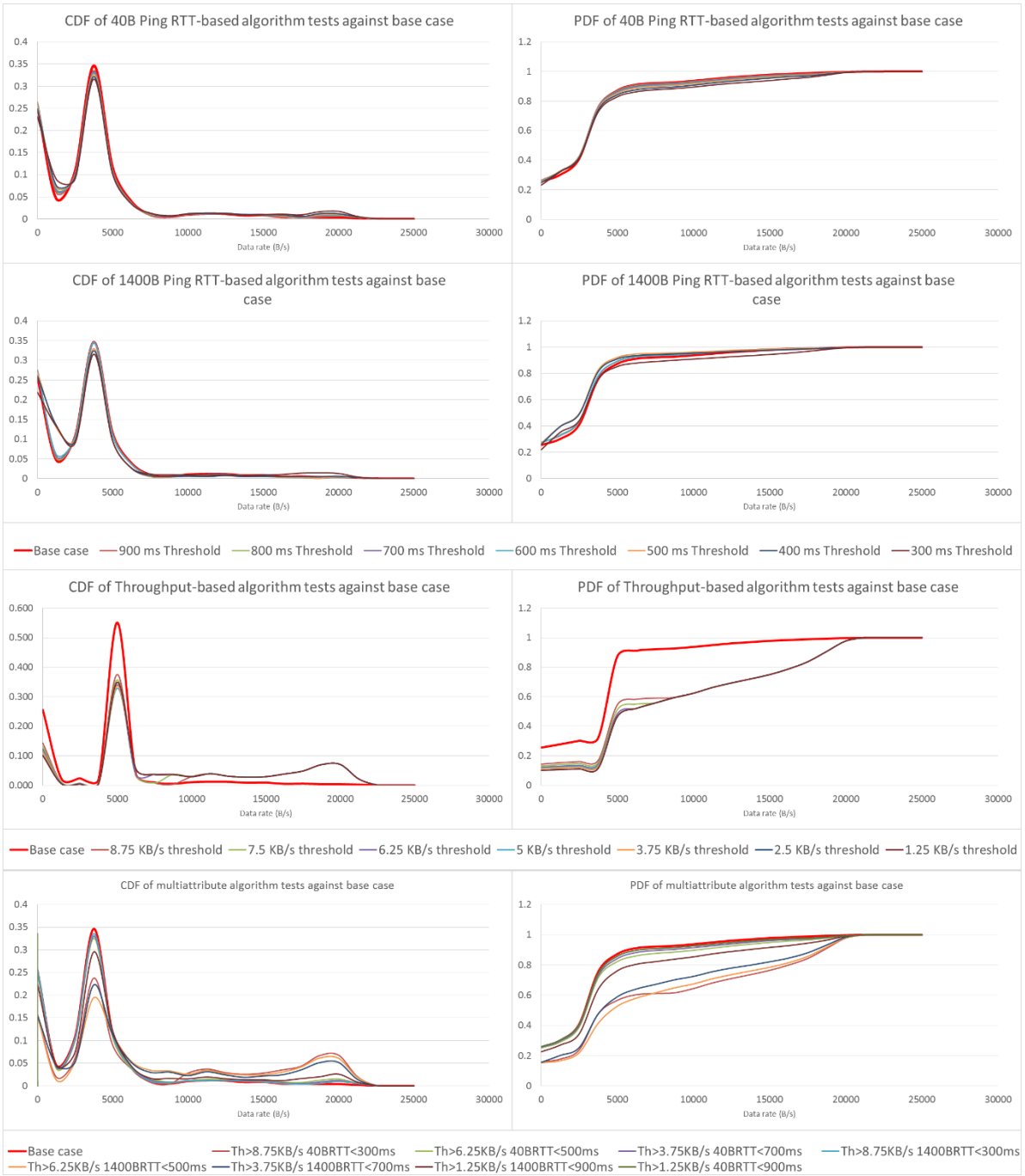

Figure 4-9 - Obtained data rate frequency distribution of the network selection algorithms.

The PDF graphs will be useful to show that the best algorithms and optimizations are the ones that will be most of the time under the base case's PDF. By itself, the 1400B RTT test provided the worst results and even increased the amount of low data rates obtained for the end user; however, when used this same ping is used as part of the multi-attribute algorithm, it is clear the resulting higher data rates increase in frequency. As a result of its inherit

qualities, all of the immediate throughput-based algorithm tests obtained better results than that of the base case.

Another way to qualify the algorithms is by how much data is needed to be transferred in order to make the network selection algorithm, this is shown in Figure 4-10, where clearly after all the tests the throughput-based algorithm is the highest consumer of data with both interfaces transferring more than 1400MB of information throughout the testing period. RTT-based algorithms clearly require less data to be transmitted or received, with 1400B pings making use of at most 10MB in an interface. One important aspect is that for the multi-attribute algorithm, total data consumption was always lower than the throughput-based algorithm and by the end of the test period, one of the interfaces consumed 380 MB of data, resulting in less than 1000MB of transmitted data.

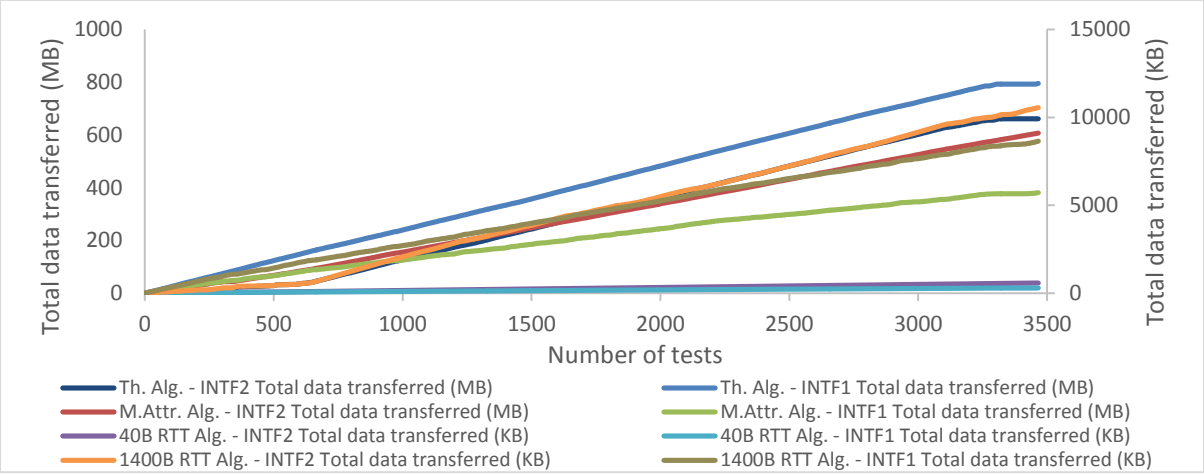

Figure 4-10 - Data consumption by network selection algorithms

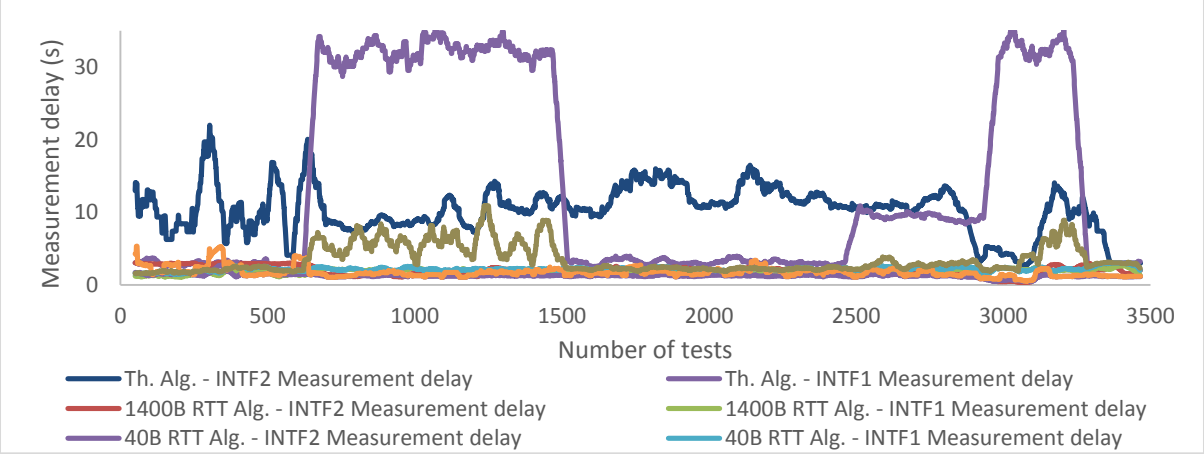

Figure 4-11 - Measurement delay in each network selection algorithm.

The final aspect that we will use to judge the proposed algorithms is by the amount of time it takes on average to get the information necessary in order to make a network selection. It's clear from Figure 4-11 that the throughput-based algorithm requires the longest time on average and this is because its network selection process requires the download of a file every time an action needs to be taken, as opposed to the multi-attribute algorithm where only if

ICMP pings are responding or the values are worse than a given threshold, there will be the need to download a file to get the throughput. In most of the cases; however, the RTT-based schemes can respond much faster when there is the need to make a network selection.

In summary, the Table 4-1 below offers the aspects in which each algorithm is more useful for the given scenarios. It's important to notice that the optimization parameters will most likely vary by terminal or by area unless a low enough value is found that can be used for a group of users.

Table 4-1 - Summary of Network Selection mechanisms

Algorithm	Pros	Cons
MIP-based	1. No additional data transfers needed. 2. Fastest handover execution as is built into the terminal.	1. Data rate is not taken into account when selecting networks, available data rate is 6.25KB/s or less in 91% of the tests. 2. Will always go back to the default interface INTF2. 3. May switch to a network that has no data access.
RTT-based with 40B Ping	1. Lowest data consumption among the proposed algorithms with 6.4MB transferred. 2. Low measurement delays with an average of 1.80 seconds.	1. Data rate improvement over base case is only marginally better with 89% of tests resulting in less than 6.25KB/s.
RTT-based with 1400B Ping	1. Low measurement delay with an average of 1.93 seconds. 2. Low data consumption with 19MB transferred.	1. Data rate is lower than base case in most of the cases with 92% of the tests resulting in 6.25KB/s or less.
Throughput-based	1. Provides the highest average data rate among all cases with 53% of the tests obtaining 6.25KB/s or less data rate.	1. Highest measurement delay with an average of 12 seconds. 2. Highest data consumption with 1.45GB transferred.
Multi-attribute	1. Provides more flexibility as there are two parameters with which it can be optimized. 2. Average measurement delay of 2.62 seconds. 3. High average data rate among all cases with 77% of the tests resulting in 6.25KB/s or less.	1. High data consumption with 988MB of data transferred.

5 Conclusions

To elaborate this thesis' conclusion first we will look into the objectives analyze if we have met the project's expectations or not and why, then we will produce the final remarks to highlight different aspects of this work and finally, future work will be proposed to expand and improve different aspects.

5.1 Objective's expectations

The main objective was to make it possible for the mobile router or; as we have denoted it, the MNR, to select a network based on the best available throughput. The reasoning behind this was that the current mechanism made use of MIP to select the network; however, is not possible for Mobile IP to realize that the mobile router is located in an area with very poor data rate in any of its interfaces. We can conclude that this objective has been achieved and we help analysis with Table 4-1. In this table we can find that the throughput-based and multi-attribute algorithms succeeded in providing a higher data rate in at least 14% more opportunities than the base case with only Mobile IP. We can also argue that small pings are able to provide a marginally better level of performance that could be used on certain situations where downloading a file is not a viable option.

Regarding the secondary objectives, the first one being an attempt to reach the *Always Best Connected* paradigm it can be concluded that in order to achieve an ABC scenario, the networks should be selected based on the end user's needs and so it is impossible due to our constraints to fulfill this; however, if we limit the scope of ABC to solely optimize available bandwidth we can certainly say that most of our proposed algorithms achieve compared to using only Mobile IP. The second secondary objective being the reduction of false positives can be marked as achieved when making use of either the throughput-based or the multi-attribute algorithms, utilizing any of these two mechanisms will allow the selection of a network that undoubtedly has data access available; on the other hand, the RTT-based algorithms won't provide a significant improvement on this matter and as such this objective is not achieved when using these methods.

5.2 Final remarks

To conclude this work, it is important to understand that the values used to optimize each algorithm will most likely vary from terminal to terminal therefore it may be good practice to select a value that will affect a wide range of terminals even if it's not fully optimized to select the highest available data rate with every run of the mechanism.

Making use of a file download to obtain the immediate throughput comes at a high cost of both time (to take the measurement) and possibly money (i.e., if data is charged per KB transferred); however, it provides information of the actual data path the end user should follow for the first hops of the network thus it can be seen as a reliable mechanism to capture this data. During the process of downloading a file, the connection will be subject to all the changes in the physical environment that could detriment the end user's experience thus we can infer from a poor download rate that the connectivity was affected and so was the user.

Not having access to the information in an external device greatly diminished the scope of possibilities to use with the studied vertical handover algorithms; however, it allowed for the study of how effective are custom made measurements tools in such restricted scenarios. As an example, having access to SNR, BER and interface buffers could have; most likely, be used in some networks selection algorithm to measure the network coverage at the interface, all of this without transmitting any data.

5.3 Future work

To continue this work it may be important to collect the network algorithm results from actual driving tests in order to optimize the threshold values. Driving tests would allow to collect more statistics from different scenarios that haven't yet been considered.

For future study, it may be useful to consider introducing a server that can respond to commands and; perhaps, control the handover of the terminals from a centralized location. Even if the terminals have the same limitations, implementing a client-server protocol with TCL scripting that could force the terminals to switch networks may be taken into considerations. Additionally, if the terminals are managed from a centralized location, it could be studied how to apply a context aware algorithm in a scenario where the terminals can provide so little information about their physical whereabouts.

6 Bibliography

[1] J. Lautmann, R. Blair and A. Durai, TCL Scripting for Cisco IOS, Cisco Press, 2010.

[2] C. Perkins, "IP Mobility Support," *IETF RFC,* no. 2002, 1996.

[3] C. Perkins, "IP Mobility Support for IPv4," *IETF RFC,* no. 3344, 2002.

[4] P. Calhoun and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4," *IETF RFC,* no. 2794, 2000.

[5] G. Montenegro, "Reverse Tunneling for Mobile IP, revised," *IETF RFC,* no. 3024, 2001.

[6] C. Perkins, "IP Mobility Support for IPv4, Revised," *IETF RFC,* no. 5944, 2010.

[7] C. Perkins, "IP Encapsulation within IP," *IETF RFC,* no. 2003, 1996.

[8] P. Sangster and K. Narayan, "Internet Control Message Protocol," *IETF RFC,* no. 5792, 2010.

[9] H. Levkowetz and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices," *IETF RFC,* no. 3519, 2003.

[10] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy Mobile IPv6," *IETF RFC,* no. 5213, 2008.

[11] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," *IETF RFC,* no. 3775, 2004.

[12] T. Narten, E. Nordmark, W. Simpson and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," *IETF RFC,* no. 4861, 2007.

[13] 3GPP, "3GPP TS 29.061 version 12.9.0," 2015. [Online]. Available: http://www.3gpp.org/DynaReport/29061.htm. [Accessed April 2015].

[14] R. Wakikawa and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6," *IETF RFC,* no. 5844, 2010.

[15] "Cambridge Dictionary," [Online]. Available: http://dictionary.cambridge.org/dictionary/british/mobility. [Accessed April 2015].

[16] E. Gustafsson and A. Jonsson, "Always best connected," *Wireless Communications, IEEE,* vol. 10, no. 1, pp. 49-55, 2003.

[17] 3GPP, "3GPP TS 23.401 version 12.8.0," [Online]. Available: http://www.3gpp.org/DynaReport/23401.htm. [Accessed April 2015].

[18] GSMA, "LTE and EPC Roaming Guidelines version 10.0," 2013. [Online]. Available: http://www.gsma.com/newsroom/wp-content/uploads/2013/07/IR.88-v10.0.pdf. [Accessed April 2015].

[19] R. Droms, "Dynamic Host Configuration Protocol," *IETF RFC,* no. 2131, 1997.

[20] "Remote authentication dial-in user service server," IBM, [Online]. Available: https://www-01.ibm.com/support/knowledgecenter/ssw_aix_71/com.ibm.aix.security/radius_server.htm. [Accessed April 2015].

[21] P. Srisuresh and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," *IETF RFC,* no. 3022, 2001.

[22] Cisco, "Cisco 819 Integrated Services Routers with 3G and Wi-Fi Data Sheet," [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/datasheet_C78-728353.html. [Accessed April 2015].

[23] Cisco, "OSPF Design Guide," [Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#t5. [Accessed April 2015].

[24] Cisco, "Internetwork Design Guide -- Designing Large-Scale IP Internetworks," [Online]. Available: http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Designing_Large-Scale_IP_Internetworks. [Accessed April 2015].

[25] Cisco, "Performance Routing," [Online]. Available: http://docwiki.cisco.com/wiki/PfR:Technology_Overview. [Accessed April 2015].

[26] Cisco, "Cisco Performance Routing," [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/performance-routing-pfr/product_data_sheet0900aecd806c4ee4.html. [Accessed April 2015].

[27] C. Paquet and D. Teare, "Appendix D - Manipulating Routing Updates," in *Building Scalable Cisco Internetworks (BSCI)*, Cisco Press, 2006, pp. 3-10.

[28] Cisco, "NAT Order of Operation," [Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html.

[29] IEEE, "IEEE 802.21 Standard for Local and Metropolitan Area Networks Media Independent Handover Services," 2009.

[30] D. Corujo, C. Guimaraes, B. Santos and R. L. Aguiar, "Using an Open-Source IEEE 802.21 Implementation for Network-Based Localized Mobility Management," *Communications Magazine, IEEE,* vol. 49, no. 9, pp. 114-123, 2011.

[31] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.-H. Cheng, A. Dutta, D. Baker, M. Yajnik and D. Famolari, "IEEE 802.21: Media independent handover: Features, applicability, and realization," *Communications Magazine, IEEE,* vol. 47, no. 1, pp. 112-120, 2009.

[32] Y. Ohba, "IEEE 802.21a Status Report," 2010. [Online]. Available: http://www.ietf.org/proceedings/78/slides/hokey-2.pdf. [Accessed April 2015].

[33] 3GPP, "3GPP TS 24.312 version 12.8.0," 2015. [Online]. Available: http://www.3gpp.org/dynareport/24312.htm. [Accessed April 2015].

[34] J. Mustajärvi, J. Tervonen, S. Slotte, J. Marin and J. Reunamäki, "ANDSF Server and Client Implementation Description," TIVIT, 2012.

[35] A. T. Campbell, J. Gomez, S. Kim, C.-Y. Wan, Z. R. Turanyi and A. G. Valkó, "Comparison of IP micromobility protocols," *Wireless Communications,* vol. 9, no. 1, pp. 78-82, 2002.

[36] A. G. Valkó, "Cellular IP: a new approach to Internet host mobility," *ACM SIGCOMM Computer Communication,* vol. 29, no. 1, pp. 50-65, 1999.

[37] H. Soliman, C. Castelluccia, K. ElMalki and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," *IETF RFC,* no. 5380, 2008.

[38] H. Yumiba, K. Imai and M. Yabusaki, "IP-based IMT network platform," *Personal Communications, IEEE,* vol. 8, no. 5, pp. 18-23, 2001.

[39] S. Fernandes and A. Karmouch, "Vertical Mobility Management Architectures in Wireless Networks: A Comprehensive Survey and Future Directions," *Communications Surveys and Tutorials, IEEE,* vol. 14, no. 1, pp. 45-63, 2012.

[40] A. Ahmed, L. M. Boulahia and D. Gaïti, "Enabling vertical handover decisions in heterogeneous wireless networks: A state-of-the-art and a classification.," *Communications Surveys & Tutorials,* vol. 16, no. 2, pp. 776-811, 2014.

[41] J. Márquez-Barja, C. T. Calafate., J.-C. Cano and P. Manzoni, "An overview of vertical handover techniques: Algorithms, protocols and tools," *Computer Communications,* vol. 34, no. 8, pp. 985-997, 2011.

[42] ITU, "Considerations of horizontal handover and vertical handover," 2007. [Online]. Available: http://www.itu.int/md/dologin_md.asp?id=T05-SG19-C-0025!!MSW-E. [Accessed April 2015].

[43] M. Louta, P. Zournatzis, S. Kraounakis, P. Sarigiannidis and I. Demetropoulos, "Towards realization of the ABC vision: A comparative survey of Access Network Selection," *Computers and Communications (ISCC), 2011 IEEE Symposium,* pp. 472-477, 2011.

[44] X. Yan, Y. A. Şekercioğlu and S. Narayanan, "A survey of vertical handover decision algorithms in Fourth Generation heterogeneous wireless networks," *Computer Networks,* vol. 54, no. 11, pp. 1848-1863, 2010.

[45] K. Meriem, B. Kervella and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks," *Computer Communications ,* vol. 31, no. 10, pp. 2607-2620, 2008.

[46] Q. Wei, K. Farkas, C. Prehofer, P. Mendes and B. Plattne, "Context-aware handover using active network technology," *Computer Networks,* vol. 50, no. 15, pp. 2855-2872, 2006.

[47] T. Ahmed, K. Kyamakya and M. Ludwig, "Architecture of a context-aware vertical handover decision model and its performance analysis for GPRS-WiFi handover," *Computers and Communications, ISCC'06,* vol. 11, pp. 795-801, 2006.

[48] C. W. Lee, L. M. Chen, M. C. Chen and Y. S. Sun, "A framework of handoffs in wireless overlay networks based on mobile IPv6," *Selected Areas in Communications, IEEE Journal,* vol. 23, no. 11, pp. 2118-2128, 2005.

[49] M. Biagi, G. Tamea and R. Cusani, "Geometric cross-layer QoS parameters based seamless vertical handover procedures in presence of adaptive modulation and coding," *Vehicular Technology Conference (VTC Spring),* vol. 73, pp. 1-5, 2011.

[50] A. Calvagna and G. D. Modica, "A User Centric Analysis of Vertical Handovers," *Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots,* pp. 137-146, 2004.

[51] M. Kassar, B. Kervella and G. Pujolle, "Architecture of an intelligent inter-system handover management scheme," *Future generation communication and networking,* vol. 1, pp. 332-337, 2007.

[52] L. Mohamed, C. Leghris and A. Abdellah, "A survey and comparison study on weighting algorithms for access network selection," *Wireless On-demand Network Systems and Services (WONS), 2012 9th Annual Conference,* pp. 35-38, 2012.

[53] S. Qingyang and A. Jamalipour, "A network selection mechanism for next generation networks," *Communications, 2005. ICC 2005. 2005 IEEE International Conference,* vol. 2, pp. 1419-1422, 2005.

[54] P. Nguyen Tran and N. Boukhatem, "Comparison of MADM decision algorithms for interface selection in heterogeneous wireless networks," *Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008. 16th International Conference,* pp. 119-124, 2008.

[55] B. Bakmaz, Z. Bojkovic and M. Bakmaz, "Network selection algorithm for heterogeneous wireless environment," *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium,* pp. 1-4, 2007.

[56] B. Bakmaz, Z. Bojkovic and M. Bakmaz, "Traffic parameters influences on network selection in heterogeneous wireless environment," *Systems, Signals and Image Processing (IWSSIP), 2012 19th International Conference,* pp. 292-295, 2012.

[57] K. R. Rao, Z. S. Bojkovic and B. M. Bakmaz, "Network selection in heterogeneous environment: A step toward always best connected and served," *Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference,* vol. 1, pp. 83-92, 2013.

[58] N. Nasser, S. Guizani and E. Al-Masri, "Middleware vertical handoff manager: A neural network-based solution," *Communications, 2007. ICC'07. IEEE International Conference,* pp. 5671-5676, 2007.

[59] P. P. Bhattacharya, "Application of artificial neural network in cellular handoff management," *Conference on Computational Intelligence and Multimedia Applications, International Conference,* vol. 1, pp. 237-241, 2007.

[60] S. Horrich, S. B. Jamaa and P. Godlewski, "Adaptive vertical mobility decision in heterogeneous networks," *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference,* p. 44, 2007.

[61] V. E. Zafeiris and E. A. Giakoumakis, "An agent-based perspective to handover management in 4G networks," *Wireless Communications and Mobile Computing,* vol. 8, no. 7, pp. 927-939, 2008.

[62] A. Hasswa, N. Nasser and H. Hassanein, "Tramcar: A context-aware cross-layer architecture for next generation heterogeneous wireless networks," *Communications, 2006. ICC'06. IEEE International Conference,* vol. 1, pp. 240-245, 2006.

[63] S. Balasubramaniam and J. Indulska, "Vertical handover supporting pervasive computing in future wireless networks," *Computer Communications,* vol. 27, no. 8, pp. 708-719, 2004.

[64] Cisco, "Configuring Mobile IP," [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfmobip.html. [Accessed April 2015].

[65] TCL.TK, "TCL 8.4 manual," [Online]. Available: http://www.tcl.tk/man/tcl8.4/. [Accessed 2015 April].

[66] Cisco, "IPSec VPN WAN Design Overview," [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html. [Accessed April 2015].

[67] Information Sciences Institute, University of Southern California, "Internet Protocol," *IETF RFC,* no. 791, 1981.